2023 Ultimate
Guide to SOC 2

Best of 2022
Audit Master Class Series

Leading Edge Strategies and Tactics from Leading SOC 2 Experts and Auditors



THE ULTIMATE GUIDE TO:

Empowering a People-First SOC 2 Strategy

OSTENDIO



Introduction

Security is a top concern for organizations today, so it's no surprise that SOC 2 continues to be a highly-requested security framework.

While a SOC 2 report should demonstrate serious security, the growing demand has also created a competitive advantage for organizations. Often, when priorities shift, the potential to lose sight of the true intention can lead to sacrificing quality.

By dedicating time and empowering their people to be secure, organizations can achieve SOC 2 success without sacrificing security.

A conversational guide to SOC 2 preparation for serious security professionals

In this expert guide, information security experts and auditors pull back the curtain to give you a behind-the-scenes look into their world. This guide includes insights, anecdotes and answers to your security questions as you navigate your SOC 2 audit.

We'll Cover

1. Getting Ready for Your SOC 2 Audit
2. Managing Expectations and Educating Your Team
3. SOC 2 Automation: The Good, the Bad, the Ugly
4. SOC 2 Pitfalls
5. Advice from the Experts

Featured contributors:

Aprio

Brett Williams
National Partner

MALONEY+NOVOTNY LLC

Dale Dresch
Shareholder

360ADVANCED

John Kadechka
Practice Director

A-LIGN

Stephanie Oyler-Rankin
Vice President of Attestation Services

DGC
ACCOUNTING • TAX • ADVISORY

Tom Strickland
Principal



Prepare for Your SOC 2 with Confidence



FEATURED CONTRIBUTOR:

Stephanie Oyler-Rankin

Vice President of Attestation Services, A-LIGN

Stephanie focuses on oversight of a wide variety of assessments within the SOC Practice at A-LIGN. Stephanie manages key service delivery leadership teams, maintaining auditing standards and methodologies, and analyzing business unit metrics. Stephanie has spent several years at A-LIGN in service delivery roles from auditing and managing client engagements to overseeing audit teams and providing quality reviews of reports.

Why every organization needs a readiness assessment

We always suggest a readiness assessment. That readiness assessment is not about us implementing different things for [the client], it's about educating–educating [the business] on the criteria, educating them on the points of focus that were used to write the criteria by the AICPA.

There's a lot of information out in the world. I think it can be very overwhelming and overstimulating to a newer organization, but the importance and the value of considering compliance frameworks as you are building infrastructure and technology, just puts you so far ahead of the curve to not have to rework.

[At A-LIGN], we do take in a lot of readiness assessment work. But again, it's more so on the education of what an audit process looks like, what evidence would be acceptable, and really guiding clients to understand the true core components of why the criteria were written and the risks that are associated to those so [the organization] can hopefully mitigate [risks] as they continue to design, build, and develop.

Staying ahead of the curve, no matter your maturity level

Organizations come in and they're really, really confident in [their SOC 2 readiness assessment]. And then they start to see the evidence request list and they're questioning, "Is this really necessary? Why would we need this?"

In the state of maturity in their organization, they may not feel that it's overly important and realize as they go through major growth spurts, how nice it is to have [certain pieces of evidence and controls] done.

I think as we see organizations grow, starting as a startup SaaS product and then growing out their product portfolio really shows over the course of time they can look back and say, "Thanks for nudging me along on that, and not really letting that fall by the wayside to implement and build out."

FEATURED CONTRIBUTORS:



Dale Dresch

Shareholder, Maloney + Novotny

Dale has more than 15 years' experience in infrastructure design, systems administration, and cybersecurity. Dale has extensive experience in systems design and process implementation, disaster recovery, network architecture, and risk management.

The importance of scoping as a storytelling mechanism

With all certifications, scoping is probably the most important exercise that you can go through. For us, it's usually a discovery process. We have a questionnaire that we step through as to your size, how many employees, how many locations–the basics, then asking, what is the point of your platform? What service are you providing? What are the key elements that you want to convey to your clients when they do use your service?

All of those things align with what is supposed to be included in a SOC 2 audit, because it's about telling your story and we want to help you tell your story in as accurate and as robust a way as we possibly can when it comes to the audit.

With all certifications, scoping is probably the most important exercise that you can go through. For us, it's usually a discovery process.



John Kadechka

Practice Director, 360 Advanced

John is a licensed CPA, Shareholder and Practice Director with more than 16 years of experience performing third-party reporting and brings a wealth of knowledge on the topic of SOC audits.

How to determine if SOC 2 is right for your organization: talk with an auditor

Scoping and the discovery call is a critical part of the process. Number one, the client needs to ensure that they need a SOC 2.

There have been a few of these discovery calls [that I have joined] and after we've talked through the services they're performing, we determined that a SOC 2 probably wasn't what they actually needed. [In many cases, these clients received] due diligence questionnaires or checklists or a new client contract that said you need to have a SOC 2, but their client didn't properly understand whether or not a SOC 2 would be a fit purpose and in some cases it's not.

That's always the first step: making sure that a SOC 2 report is actually what you need and what your customers are asking for.



Managing Expectations and Educating Your Team

FEATURED CONTRIBUTOR:

Stephanie Oyler-Rankin

Vice President of Attestation Services, A-LIGN

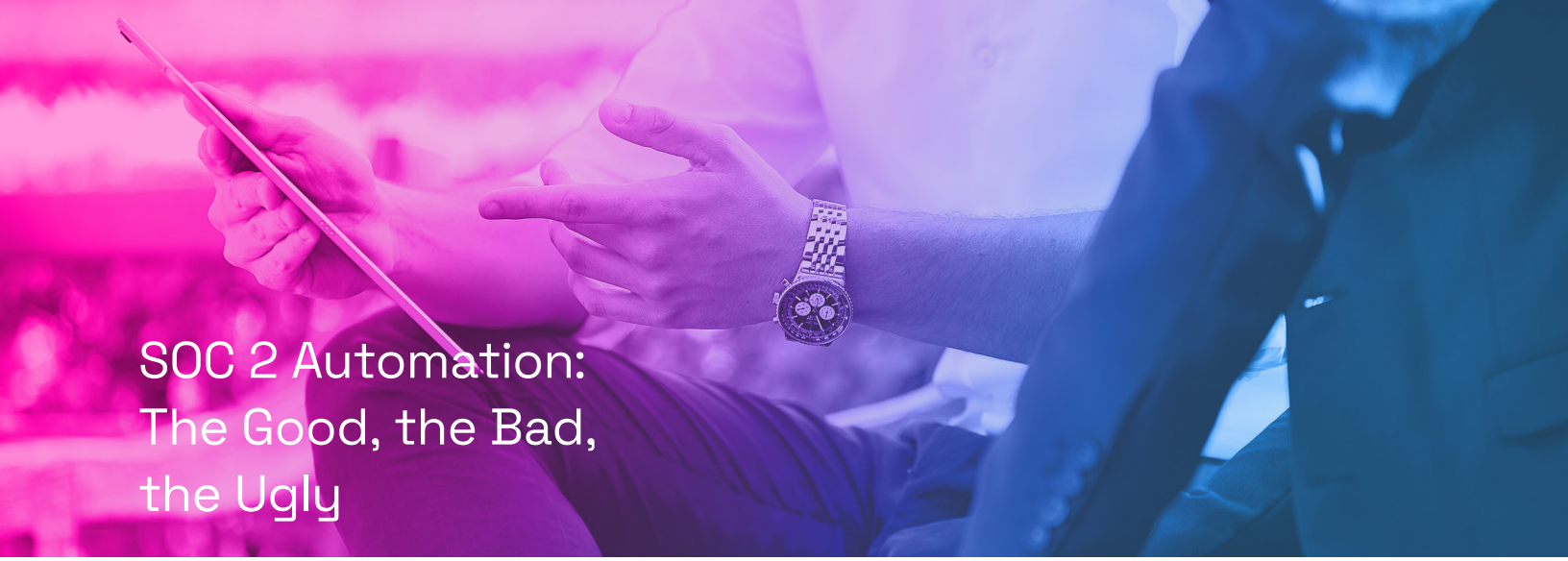
Helping your team understand realistic budget and audit delivery timelines

A lot of organizations overlook the preparation time on their own end and the cost of that–time is money. You're pulling people away from other duties if you don't have a dedicated compliance professional. It's not necessary to have a compliance professional, you know, dedicated to an audit in order to pass it, but there is a lot of time that goes into that.

So I think first and foremost, understand that a lot of those slogans that you see out on LinkedIn–they're referring to an audit process and, and they're not really referring to the process that it takes to educate yourself and to prepare your organization.

It's similar to taking a test. If you didn't spend any time studying, it's probably going to take you longer to second guess yourself during the test. If you studied and you were really well prepared, you might be the first one out of the exam room.

> There's a lot of gray matter that goes into an audit, because, if you are really treating audit as a checkbox activity in your preparation, when you get to actual audit time, it will not go as smoothly as you anticipated.
>
> **STEPHANIE OYLER-RANKIN** | A-LIGN



SOC 2 Automation: The Good, the Bad, the Ugly

FEATURED CONTRIBUTOR:

Stephanie Oyler-Rankin

Vice President of Attestation Services, A-LIGN

Replacing the gray matter of the 2-week audit process with a people-first approach

Just having a risk assessment and having a document that's titled "risk assessment" is not enough. You have to have a lot of considerations to go into risk assessment to meet that control family within the security category of a SOC 2. There are many points of focus that are written on those criteria specifically, and there's several criteria that address not only risk assessment, but risk mitigation.

Just checking the box and saying, I have a risk assessment, when it comes audit time or test time, it's not really going to hold up to those standards and those points of focus that auditors are truly testing against.

There has to be some sort of human interaction there because most organizations are still employing people and still providing services or products to human beings. There's just naturally always going to be some sort of gray factor in there that can't be fully automated and that's where true preparation and understanding that a 2-week audit process is really not going to be able to dive into that gray matter and assess all of the other aspects of an organization beyond just technology.

Overlooking that piece can be a little dangerous, but we have a lot of clients that come to us and say, "Can this happen? Is this possible?" And, and we go into those facts there's an organization and management system piece that goes to SOC 2, and understanding that it takes people to onboard people, to make people understand the risk around open emails.

A lot of factors come into play whenever you add human beings into interactions. I don't know many companies that are operating without people.



FEATURED CONTRIBUTOR:

Brett Williams

National Partner, Aprio

Brett is a licensed CPA with expertise in the evaluation and design of vendor management programs. Brett has more than 20 years of experience, has performed more than 3,000 audit and compliance engagements for small to midsize companies in fintech, healthcare IT, technology, insurance, and more.

Resist check-the-box audits: customizing your SOC 2 to your people and your business

The point [of the SOC 2 audit] is to make a unique control for your environment. Everybody doesn't have the [same controls]. So a lot of times what you'll see with what I call a "check the box audit" is every control is the same for every single one of the clients.

I don't care if you're in AWS (Amazon Web Services), and you're still a SaaS platform–your controls are different. How you implement change management is different. Maybe your infrastructure is a code, maybe it's not.

[Your SOC 2 report] should not be identical to your neighbor who bought the same product. It takes a lot of time to customize that, and it makes the report so much more useful, not just for you internally, but when you hand it out to your customer and they actually ask questions and read those controls. They're actually reading your controls and not just some generic thing that is everybody else.

Key Takeaways from Aprio

- **Not all organizations are created equal**
  Your business is unique from every other business, and Yutomation puts you in a box that won't necessarily fit your organization's security and compliance needs.
- **Customizing SOC 2 to your organization is effective**
  Not only from a compliance standpoint, but from a security perspective.
- **Customizing your SOC 2 demonstrates that you take security seriously**
  And when you take security seriously, you demonstrate to your clients, partners and stakeholders that your organization is accountable and trustworthy.



FEATURED CONTRIBUTOR:

John Kadechka

Practice Director, 360 Advanced

3 Questions you can ask to help identify if your SOC 2 is the real deal

Is [the audit] complete, is [the audit] accurate? How much reliance are we putting on it? How critical or how high of a risk is the control that's using that data and going through all these factors? And that should really then assess how robust the auditor's really going to dig into the completeness and the accuracy of that data as well, based upon the criticality of that control and of that key report.

I think that's one of the areas that maybe some of the check the box firms really aren't digging into–the completeness and the accuracy of the data that's either used by us as the auditor, or as a population.

Top Takeaways from 360 Advanced

- **If you automate your SOC 2**
  Ask yourself how much reliance you're putting on it.
- **Automating SOC 2 doesn't necessarily mean it's complete or accurate**
  In most cases, it's not. Make sure your auditor is asking the right questions to dig into the integrity of your report so no stone is left unturned.
- **Check that your organization is comfortable with the outcome**
  Is the data being collected and used accurately to depict your organization's compliance and security?

FEATURED CONTRIBUTOR:

Dale Dresch

Shareholder, Maloney + Novotny

How to determine if automating your SOC 2 puts your organization's compliance at risk

It's people, process and technology. The technology might be working correctly, but maybe it doesn't fit necessarily into the process of the people. So, just because you have a green icon on your screen saying it's compliant, it doesn't necessarily make it compliant.

It's [an auditor's] job. We go into these things as far as we can to make sure that they actually are working the way that they should. Sometimes yes, it says it's compliant, but it doesn't necessarily mean it's fulfilling all of the criteria or all the points of focus for that defined criteria.

FEATURED CONTRIBUTOR:

Brett Williams

National Partner, Aprio

I need to get certified fast–can it be done, and is it worth it?

If you're a really small software as a service company, you might be able to say you can do something in a certain time period. But if you're in a cloud environment, maybe a multi-cloud environment, and you have multiple databases, multiple applications–it's really hard.

The reality is there's always going to be give and take. [You're always going to be trying] to understand the documentation. There's always going to be something that's needed over and beyond what you might be able to automate.

I think that's kind of a misnomer. It's never "hit the button." It would be great to hit the button, and maybe someday that will be the case. But, you're going to have different people reviewing this information and asking questions. And even if it is exactly what we need, it's not going to be necessarily question-free when we look at it.

> "There's always going to be something that's needed over and beyond what you might be able to automate.
>
> **BRETT WILLIAMS** | Aprio



SOC 2 Pitfalls



FEATURED CONTRIBUTOR:

Tom Strickland

Principal, DGC, a Devision of PKP O'Connor Davies

Tom has over 17 years of experience in internal and external audit in the technology space, with the last 5 in a managerial capacity with a concentrated focus in Information Security. Tom is graduate of Bentley University and is a Certified Information Systems Security Professional, Certified Information Systems Auditor and an AWS certified Cloud Practitioner.

Areas of importance you never want to overlook

[Risk assessment] is an area that's a common pitfall for organizations in a SOC 2. Organizations are handed, "Here are your risks," and it's 10-15 risks that may or may not apply to the organization. That's not the best approach. Ultimately, it comes down to having the right people, and obviously the right processes.

Some of the other common pitfalls that I often see are around third party due diligence. That is an area where maybe the organization just misunderstands the requirements. They're not performing the necessary due diligence at a level that's maybe required to meet the criteria. What's the root cause? Maybe it's because they don't have the resources in-house or maybe they just don't have the experience.

Common pitfalls to always have on your radar:

- **Don't take risks at face value**
  Understand what your unique risks are and work with your team to identify them. Avoid accepting blanketed risks from a company as they may not necessarily fit into your business.

- **Take security seriously**
  Don't provide arbitrary evidence or only perform security measures halfway. An auditor will likely test all components of evidence to ensure the security measure is performed diligently without skipping steps.



SOC 2 Advice from the Experts

FEATURED CONTRIBUTOR:

John Kadechka

Practice Director, 360 Advanced

Why your SOC 2 report needs boundaries

After we've determined that [the organization] needs a SOC 2, it's clear for management to understand what specific services they're providing.

One of the things that we try to do in these early discovery and scoping calls is try to put a fence around what the system boundaries that the SOC 2 defines–talking through the infrastructure, the data, the applications, the people, all the components really so that we can put a fence around it.

A client may start talking about specific areas that right away I can say that likely would not be relevant to your users–and we probably don't need to bring that into the scope of the SOC 2. Putting a fence around the boundaries and what's going be brought in is critical to performing a SOC 2 report.

FEATURED CONTRIBUTOR:

Stephanie Oyler-Rankin

Vice President of Attestation Services, A-LIGN

What to expect if you receive an unqualified report

[Failing an audit] does unfortunately happen at times. When we identify a problem in an audit, we are immediately talking to the client about that problem to gain an understanding of what the issue is. First and foremost, we try to get a full understanding of what is happening and if the client is aware that it's a risk, are they willing to accept if they choose to mitigate in different ways or if it's something that maybe they are actively working on.

Sometimes [those clients] don't find that comforting and they will then go through another audit. They'll clean up whatever the issue was, and sometimes they'll do an interim Type 1 report, or maybe Type 2 that only covers maybe a 6-month review period. We have seen that happen every once in a while. A lot of times, we'll build out additional materials and provide it to clients to show that those gaps have been patched and taken care of. Then, we revisit the audit cycle maybe a little bit earlier in the following year.

FEATURED CONTRIBUTOR:

John Kadechka

Practice Director, 360 Advanced

Don't underestimate setting realistic expectations, and understand your audit will change year-over-year

Management always needs to make sure that they understand what the time commitments are. With a first year report, there's always going to be a bit more that's needed. The walk-throughs are going to be a bit more detailed because it's us gaining our understanding of your environment and you also getting a feel for us as well, too.

If we're going from year one and year two then into year three, we always have to add unpredictability to our audit procedures. The way that we audited one thing this year is going to have to change because the AICPA requires that we try to add unpredictability year over year so that our clients aren't expecting the questions that we're going ask or expecting the type of evidence that we're going to ask for.

> We have to get a bit creative on our end as well, and try to add a bit of that unpredictability into our procedures year over year.
>
> **JOHN KADECHKA | 360 Advanced**



Conclusion

Additional SOC 2 Resources:

Click the links below for more SOC 2 information

- Ebook: The Complete Guide to SOC 2 Audits
- SOC Audit Master Class Part 1: Get in Shape for Your Next SOC 2 Audit
- Audit Master Class Part 2: SOC Secrets of Success
- The Rise and Fall of SOC 2 Audits
- Why Preparing for a SOC Audit Takes More Than 2 Weeks

Everyone Secure.

Welcome to the next generation of security.

Ostendio is the only risk management platform that leverages the strength of your greatest asset. Your people. With deep customization, advanced intelligence, and flexible controls, you're always audit-ready, always secure, and always able to take on what's next.

Schedule a demo today.

Authorized licensee for SOC1®, SOC2® & SOC3®
Used under license by AICPA

HITRUST
Authorized Readiness Licensee