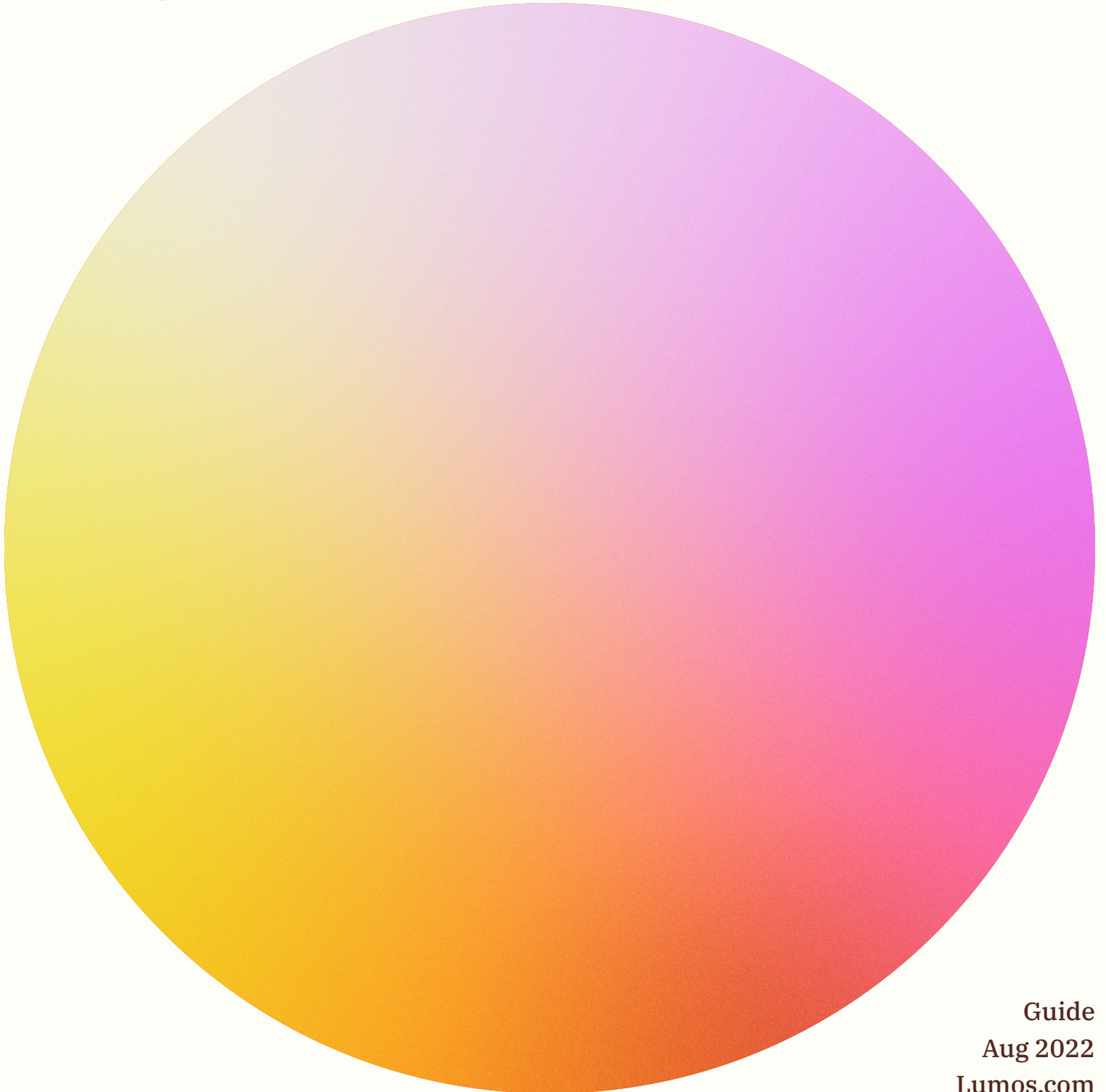


# From Start to Certificate: A Practitioner's Guide to SOC 2 Compliance

By Alan Flores Lopez  
Co-Founder @Lumos



Guide  
Aug 2022  
Lumos.com

SOC2 compliance. Those words are often enough to send a shudder down a spine. There's no clear step-by-step guide and the process takes months to complete.

**But it doesn't have to be that way.**

I'm Alan Flores Lopez, co-founder at Lumos. Recently, Lumos went through an audit period for our SOC 2 compliance certificate. We learned a lot and found ways to be more efficient and meaningful, particularly for the system access control and vendor management policies.

Here's our hands-on roadmap to help you whittle down the workload, simplify the process, and easily finish your SOC 2 audit.

# Compliance

## Choose Your Approach

There are a few ways to approach SOC 2 compliance. Getting the certificate can be a chore if you simply want to check boxes. Or, it can be an opportunity to improve your company's security and compliance policies and procedures.

Remember SOC2 compliance is subjective — it's your job to tell the auditor how you're satisfying the criteria. Everything must align with your business objectives. And that's why we created our security, trust, and system design framework. This helped us understand why we were implementing certain policies and procedures, which allowed us to design a process that made sense for our company and our customers.

### Here's our foundation:

**Security:** Are we actually mitigating security risk? Is this a meaningful practice that improves technical and organization system design?

**Trust:** Are we approaching compliance in a way that makes customers trust us with their data? **SOC 2 is a formalized way of earning this trust**, but not the only way. Security questionnaires, emails, Slack, and meetings should all be considered when approaching SOC 2 policies.

**System Organization And Design:** Good organization and least privilege makes it less likely that we will have outages because of any mistakes.

## Create Your Network

Google is certainly helpful, but an internet search for SOC2 compliance doesn't exactly give you a solid starting point. Rather than spending hours searching the web, talk to people who have done it before. Or, find a partner, such as Vanta, Drata, or Secureframe. We used Vanta. They provided guidance, templates, frameworks, auditor information, and process overviews, saving us time and sanity.

---

**The network effect: Advisors, investors, and other experts in your network can provide valuable information about auditors, processes, and what customers want.**

---

Your auditor will play a huge role in your SOC 2 journey—they can really make or break the experience. If you use a partner, they will have auditor recommendations. Regardless, choose one that listens, responds quickly, and fits your needs and budget. Don't overshoot. And build that relationship. This will help you get detailed answers and make sure you are both aligned on control language.

---

**The writing's on the web: Companies often make SOC 2 audits public, which can help you understand different auditors—and what they might expect.**

---



## Choose Your Categories

Once you've chosen your auditor, you can select which of the five SOC 2 Trust Services categories make the most sense for your company. Security and availability are the most common. On the advice of our auditor, we also chose privacy.

Here's a list of the Trust Services categories:

**Security:** This principle gives a customer reasonable assurance that their data is safe and secure, and demonstrates that systems are protected against unauthorized access (both physical and logical).

**Availability:** Besides the security principle, availability is the second most common principle chosen for the SOC 2 examination. It focuses on systems being available for operation and use.

**Processing Integrity:** This principle focuses on system processing being complete, accurate, timely, and valid.

**Confidentiality:** The confidentiality principle ensures information deemed confidential is protected as committed or agreed.

**Privacy:** The privacy principle refers to how personal information (first name, last name, address, phone number, etc.) is collected, used, retained, disclosed, and disposed of. It ensures your data handling practices align with your privacy notice and use the criteria defined in privacy principles issued by the AICPA.

Before you choose your Trust Services categories, do a pulse check with your sales pipeline. Your potential customers will tell you which categories influence their purchasing decisions. By focusing on what your customers want, you'll avoid the trap of choosing categories that aren't yet relevant for your company.

## Get Organized

Now the real fun (and work!) begins. Being organized is half the battle—but it's only easy if you have the right tools in place. Most importantly, make sure you have one single source for information. Then, let the policies dictate everything you do. Use the templates you have and any checklists your partner provides.

We translated policy language to processes in Notion pages. This allowed us to keep track of evidence and easily export to PDFs when fulfilling audit requests.

As a general rule, this is the overall process we followed for all policies to make sure we were on track before the observation period.

- **Assign Stakeholders:** Clearly designate task owners from IT, engineering, operations, and management. Who is responsible for what? How do they do it?
- **Create a compliance calendar to stay on track.**
- **Build Your Infrastructure:** We used Notion to consolidate information because it's centralized and has version control.
- **Define your process:** Have weekly and monthly status checks. By the time we got to the observation period we really had this nailed down. I've included our step-by-step guide in the preparedness packet download at the end of the article.

This includes manual reviews of IAM access and security groups, automated checks of AWS, backups and versioning, up-to-date utility hosts, external security advisories, and more.

With Lumos and Notion, our vendor risk assessment, access requests, and on and offboarding are all updated and available in real time. We don't need to perform manual reviews or adjustments.

---

**Download the SOC 2 Resource Kit [Here](#)**

---

Don't like it? Keep doing it. Difficult processes become easier over time.

Always look for ways to calibrate and refine. You'll uncover new ways to automate as you go.

These processes were helpful for all policies. But System Access Control and Vendor Management required the most information gathering—and are traditionally the most difficult to manage. Auditors want to see a lot of documentation for how a company manages app permissions, access reviews, on and offboarding, and vendor risk assessments. Both components have a number of moving pieces and can change quickly as employees or vendors are added, changed, or removed.

**At Lumos**, we build technology that helps companies manage and automate system access control and vendor risk assessment. We used our own tools for this part of the audit, and those tools enabled us to provide the information without the typical heavy lift. Lumos pulls all of this data into one interface—so we spent time creating and refining our process rather than swimming in spreadsheets. During the audit we could easily grab relevant information and compile it into an auditor-friendly PDF.

**Lumos works well for smaller companies like us, but the value increases as companies grow.** More apps plus more users equals more to track. Lumos helps tame the app and permissions sprawl.

Here's what we did:




## Role-Based Permissions

First, we created and defined employee roles and scopes and compiled those into a list. This became our blueprint from which to work. We update our list quarterly. The list helps us enforce role-based access control, which is important for our foundation of trust, security, and organization system design. Lumos shows us all of the applications we are currently using so we can set the right permissions. From there, we determine who has access to which applications—and how much access they need.



We don't maintain spreadsheets for system access control because we don't need to. All information is always up-to-date and available within Lumos, including access requests and on/offboarding information.

## Roles \*\*\*

 Name	 Description	 Permitted apps/roles
<b>Base Full-Time</b>	Base access for all non-contractor Lumos employees	Base access to core tools: Slack, Google, Lumos, Notion, Zoom, Loom, Productboard, Figma, Asana, Calendly, Miro, Rippling, Greenhouse  Discretion-based access to the Lumos identity dashboard as admins.
<b>Base Contractor</b>	Base access for Lumos contractors	Access to restricted channels on Slack
<b>Recruiter Contractor</b>	Contractor that helps with recruiting efforts.	Access to Greenhouse, Gem, Slack, Email
<b>Engineering Contractor</b>	Can develop against a subset of the Lumos application, with some access to development infrastructure.	Select GitHub Repos. Select Notion pages. AWS account with restricted access and some development data read access.
<b>Future Employee</b>	An employee that has signed an employment contract but whose start date has not begun.	Base access to Google Workspace, Slack, Notion, Pitch, Productboard, Asana so that they may begin to read context about Lumos.
<b>Future Engineer</b>	An engineering employee that has signed an employment contract but whose start date has not begun.	Same access as future employee, but also read access to the Github repo, as well as regular access to Figma for designs.
<b>Software Engineer</b>	Design and develop the Lumos product.	Everything in the Base Full-Time role plus the following:  Basic access to: Datadog, Github, Pagerduty, AWS, Sentry, CircleCI, Jumphost (selective)

## Access Request Policy Language

Requests should be made to people who manage the relevant resources, they are made by employees or their manager, do not grant root access, ensure grants are scoped to minimum breadth / duration, people must read and accept Acceptable User Policy during onboarding.

## Access Requests

Access requests are important for maintaining least privilege access and compliance. Without these requests there are no logs or any criteria for business-justified access. Or worse, everyone has open access. App access should be tightly controlled and every company should have an audit trail showing requests and permissions granted.

**At Lumos**, we centralize and manage access requests for all SaaS apps. All access requests run through Slack and Lumos tracks permissions granted in the platform.


Requests get directed to the approver or app admin to approve and complete provisioning. Lumos and Slack make it easy for our users to find an app and request access or a permissions change—and easy for us to track for the audit.

## On And Off-Boarding

Giving new employees app access quickly allows them to be productive sooner. But revoking access is critical when employees move on from the company. In Lumos we can off-board them with just one click (really!). This immediately revokes any access they had to company applications. For example Lumos is smart enough to understand that removal from Google Workspace prevents Google OAuth sign in to other applications.

## Vendor Management

The vendor management policy provides a framework for companies to manage the lifecycle of vendor relationships. It’s a standard security and compliance process—and something your customers will care about. Our management process includes an extensive list of all vendors, associated risk rankings, and data from the most recent evaluation.

 **Vendor Risk Assessments**

Default view

High Risk Only

Medium Risk Only

Low Risk Only

Vendor	Risk	Actively Used	Approved by IT team	Vendor Sponsor	Last Updated At	Annual Cost (\$)	Contract Length
Google	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:51 PM		
Zoom		<input type="checkbox"/>	<input type="checkbox"/>		January 17, 2022 10:14 PM		
Slack	Medium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		March 9, 2022 2:06 AM		
Microsoft	Low	<input type="checkbox"/>	<input checked="" type="checkbox"/>		April 8, 2022 5:13 PM		
Dropbox	Medium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		January 30, 2022 4:25 PM		
Zoom	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		January 22, 2022 7:03 PM		
Asana	Medium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		January 30, 2022 4:26 PM		
Atlassian	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		January 30, 2022 4:26 PM		
AWS	High	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		January 30, 2022 4:27 PM		
Zoom	Medium	<input type="checkbox"/>	<input checked="" type="checkbox"/>		January 30, 2022 4:32 PM		
Zoom	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		January 22, 2022 8:35 PM		
Zoom		<input type="checkbox"/>	<input type="checkbox"/>		January 17, 2022 10:16 PM		
Zoom	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		January 30, 2022 4:32 PM		
Zoom		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		January 30, 2022 4:40 PM		

COUNT 126

## Vendor Management Policy Language

A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.

## Vendor Risk Assessment

Every vendor we use has an internal vendor sponsor who acts as a liaison between the vendor and Lumos. Our internal process for assessing vendor risk goes like this:

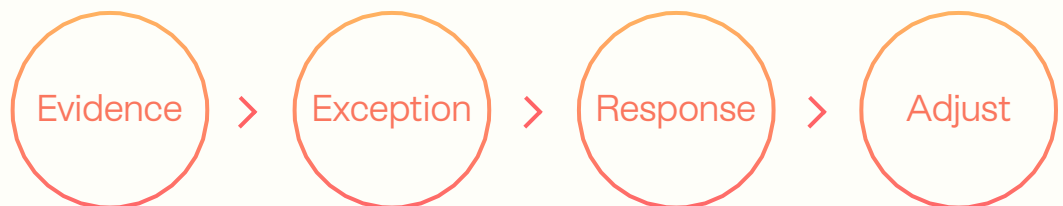
- On Slack, someone posts an app request in **#vendor\_requests**
- We create an entry for that app in Notion and ask the person to fill in some details.
- We assign an app sponsor.
- The sponsor completes a vendor services description form that is tied to a risk assessment matrix we created.
- The sponsor performs any due diligence, fills in the risk assessment on the Notion card, and approves the request.
- The sponsor then re-evaluates the vendor after initial procurement and continues to do so every year.

We can use Lumos to find applications that are not currently in our spreadsheet, including new apps or apps we no longer use. Lumos also helps during the annual audit because we can see which vendors aren't included in our vendor review cycle.

## Pass The Test

Once you're ready to go your auditor will begin the observation period. They'll want evidence and controls relating to your Trust Services categories. Screenshots or PDF documents with appropriate timestamps usually work.

The audit isn't necessarily pass or fail. Your auditor will give you an exception for any process that doesn't match up with the controls. You'll then have the opportunity to respond and adjust.



Here's how we provided evidence for system access control and vendor management:

### Access Requests

Since all access requests are automatically routed through Lumos and our Slackbot, all I had to do during the audit was share my screen. I could have also easily shown the audit log in Lumos, if needed, but the Slackbot channel showing the requests was enough to satisfy the requirements.

## On And Offboarding

Every user has a page in Lumos that shows current access or any deprovisioning, so we simply shared screenshots of those pages as SOC2 evidence.

## Vendor Management

The auditors focused primarily on the date of last review, approval or denial of continued vendor relationship, and any open action items. We were audited on how we performed our annual vendor reviews, but we didn't need to show our process for documenting any significant vendor relationship changes. I simply provided a PDF of our Notion page as supporting evidence of how we manage our vendor risk.

* Vendor Risk Assessments							
[Default view] [High Risk Only] [Medium Risk Only] [Low Risk Only]							
Vendor	Risk	Actively Used	Approved by IT team	Vendor Sponsor	Last Updated At	Annual Cost (\$)	Contract Length
Google	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:51 PM		
Zoom		<input type="checkbox"/>	<input type="checkbox"/>	Andrej Safundzic	January 17, 2022 10:14 PM		
Slack	Medium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	March 9, 2022 2:06 AM		
Dropbox	Low	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	April 8, 2022 5:13 PM		
Microsoft	Medium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:25 PM		
Zoom	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 22, 2022 7:03 PM		
Asana	Medium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:26 PM		
Atlassian	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:26 PM		
AWS	High	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:27 PM		
Zoom	Medium	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:32 PM		
Zoom	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 22, 2022 8:35 PM		
Zoom		<input type="checkbox"/>	<input type="checkbox"/>	Andrej Safundzic	January 17, 2022 10:16 PM		
Zoom	Low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:32 PM		
Zoom		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Andrej Safundzic	January 30, 2022 4:32 PM		
COUNT 126							



## The Path Forward

SOC 2 audits don't stop when the observation period ends. You have to continually show your work. And the ongoing process is no different than the initial audit. So make it meaningful. Set tasks to make sure additional reviews are done. Learn what your customers want. Keep your team engaged so they continue to build compliance muscles.

And remember, continuous compliance requires continuous updates, so those once accurate spreadsheets are quickly out-of-date. Lumos makes sure your on/offboarding, access reviews, and vendor risk assessments are always up-to-date.

I hope this SOC 2 guide helps you decide on what security and compliance look like for your company and that it helps you navigate some of the harder parts of the audit. Best of luck as you go through the audit process!

---

Download the SOC 2 Resource Kit [Here](#)

---



## On And Offboarding

Alan is the co-founder of Lumos. Alan received his MS and BS in Computer Science from Stanford. Previously, he was a security engineer at Samsara. Before that, he ran Stanford's cybersecurity course under Prof. Dan Boneh and interned at Pinterest and Microsoft. Alan likes to read (usually about film & media), practice classical guitar, and listen to prog rock.

Follow Alan on [LinkedIn](#)



## About Lumos

Employees shouldn't be admins for hundreds of web apps with excessive permissions. But then again, nobody wants to be stuck in IT ticket queues for days to get the right access. With Lumos, you make your company more productive and compliant with self-service app requests, access reviews, and license removals.

[Click here to try Lumos out](#)

# From Start To Certificate: A Practitioner's Guide To SOC 2 Compliance

