KirkpatrickPrice

SOC 2 Checklist

Preparing for Your SOC 2 Audit

A SOC 2 report is an attestation that the system or service you provide to your clients is secure, trustworthy, and prepared to handle risks. A SOC 2 report validates your organization's commitment to delivering high quality, secure services to your clients.

A SOC 2 audit provides this assurance by evaluating the controls that directly relate to the AICPA's Trust Services Criteria. This means that a SOC 2 audit report focuses on a service organization's internal controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.

It is important to note that compliance is not achieved by completing a checklist; however, this checklist will prepare your organization to meet the requirements of the SOC 2 framework. A SOC 2 has predefined criteria (the Trust Services Criteria) that must be met, but how your organization meets those requirements is up to you. An audit with KirkpatrickPrice will ensure that the controls you have implemented meet the requirements of a SOC 2 audit and provide your organization with confidence in the effectiveness of those controls.

Frequently Asked Questions

What system components are evaluated during a SOC 2 audit?

- **Infrastructure** - physical, IT, or other hardware such as mobile devices
- **Software** - application programs and IT system software that supports application programs, such as OS and utilities
- **People** - all personnel involved in the use of the system
- **Processes** - all automated and manual procedures
- **Data** - transmission streams, files, databases, tables, and output used or processed by a system

What are your auditors looking for?

- A fairly presented description of a service organization's system relevant to one or more of the Trust Services Criteria
- Design and operating effectiveness of a service organization's controls over a system relevant to one or more of the Trust Services Criteria

How long does a SOC 2 audit take to complete?

The average SOC 2 audit, using KirkpatrickPrice's process, is completed in 12 weeks. The engagement begins with scoping procedures, then moves into an onsite visit, evidence review, report writing, and concludes with the delivery of a SOC 2 report. This timeline is extended when a gap analysis must be performed or when remediation takes longer than expected.

Who can perform a SOC 2 audit?

A SOC 2 audit can only be performed by an auditor at a licensed CPA firm, specifically one that specializes in information security. SOC 2 audits are regulated by the AICPA.

Compliance Guidance

This checklist includes all of the system components that are evaluated during a SOC 2 audit. Use this checklist to learn what your auditors are looking for and how to prepare for your SOC 2 compliance audit.

Keep in mind, you don't have to have everything perfectly in place to start your audit; this checklist should just be a tool to help you prepare for your audit. If you need help putting any of these controls in place, contact one of our experts today! We want to make sure you feel ready to successfully complete your SOC 2 audit!

SOC 2 Checklist

- [ ] A defined organizational structure is implemented
- [ ] Authorized employees have been designated to develop and implement policies and procedures
- [ ] Background screening procedures are in place
- [ ] Workforce conduct standards are established
- [ ] Clients and employees understand their role in using your system or service
- [ ] System changes are effectively communicated to the appropriate personnel in a timely manner
- [ ] A Risk Assessment is performed at least annually
  - [ ] Potential threats to the system have been identified
  - [ ] The significance of the risks associated with each threat has been analyzed
  - [ ] Mitigation strategies for those risks have been developed
- [ ] Regular vendor management assessments are performed
- [ ] All organizational controls are documented with policies and procedures
- [ ] Policies and procedures are reviewed at least annually
- [ ] Physical and logical access controls are in place
- [ ] Access to data, software, functions, and other IT resources is limited to authorized personnel based on roles
- [ ] Physical access to sensitive locations is restricted to authorized personnel only.
- [ ] An access control system, as well as monitoring to identify intrusions, has been implemented
- [ ] Incident response procedures have been developed and tested
- [ ] Software, hardware, and infrastructure is updated regularly as necessary
- [ ] A change management process to address deficiencies in controls is in place
- [ ] Backup and recovery policies are in place
- [ ] Environmental risks have been addressed
- [ ] Your disaster recovery plan has been tested and documented
- [ ] Data is being processed, stored, and maintained accurately and timely
- [ ] Confidential information is protected against unauthorized access, use, and disclosure
- [ ] A fully documented data retention policy is in place

Audits are hard.
We make sure they're worth it.

At KirkpatrickPrice, we know that when it comes to threats you want to make sure that you're ready. In order to do that, you need quality cybersecurity and compliance audit reports with results you can trust. The problem is SOC 2 audits are hard because the process is complicated and feels overwhelming. We believe if you're going to do it, the audit should be worth it. We've been in your shoes and know how hard audits can be, but we've issued over 20,000 reports to 2,000 clients worldwide, giving them the assurance they deserve.

When you work with KirkpatrickPrice, you can stop feeling you are going to miss something or be surprised when a client or attacker finds something that wasn't in your report. You can stop feeling worried that you're wasting your time using someone who's not advanced enough to thoroughly test your environment. Instead, you'll have a report that gets you ready for your next steps, allows you to say yes to client requests, and brings you the assurance you deserve. Cybersecurity and compliance will no longer be a mystery.

To get started on your SOC 2 audit, call one of our experts today at 800-770-2701 or visit www.kirkpatrickprice.com.