Prevalent™

How to Use SOC 2® Reports to Assess Third-Party Risk

8 FAQs and tips for using SOC 2 reports to simplify your vendor and supplier risk management program

Table of Contents

What is a SOC report, and how is it used?

System and Organization Controls (SOC) is a set of IT controls standards developed by the American Institute of Certified Public Accountants (AICPA). SOC audits are performed by certified auditors, and reports are used to demonstrate how IT controls have been implemented to secure a company's systems and information.

SOC reports provide detailed assessments of an organization's operations and systems, and their effectiveness.

Organizations undertake SOC audits to prove that they are building a structured framework for identifying and assessing risk; demonstrating the design and effectiveness of security and privacy controls; and providing key stakeholders with confidence that security and privacy best practices are being followed.

There are two types of SOC reports:

- **Type 1 reports** review the design of security controls, including procedures and processes. Type 1 audits are conducted at a single point in time.
- **Type 2 reports** review the operational effectiveness of the controls identified in Type 1 reports. Type 2 audits look at controls in depth and are conducted by auditors over a longer period of time – sometimes as long as six months.

This e-book focuses on SOC 2 Type 2 reports.

SOC audits are built to assess controls in five key areas, called **Trust Services Criteria**.

1. **Security**
2. **Confidentiality**
3. **Processing Integrity**
4. **Availability**
5. **Privacy**

What do SOC 2 reports contain?

While SOC 2 reports can look different based on the auditor conducting the assessment, they generally include the following areas meant to identify the scope of the assessment and non-conformities, known as control exceptions.

- **Executive or auditor summary:** Includes an overview of audit results, how the auditor conducted the audit, and some level of guidance indicating whether findings are more or less relevant.
- **Overview of organizational operations, processes and systems:** Reviews the organization and its audit objectives.
- **Scope of the report:** Examines the five Trust Services Criteria and supporting controls in scope for the audit. Sometimes, organizations choose to only focus on one or two Trust Services Criteria instead of all five, especially if some of the criteria don't apply to them.
- **Control activities and auditor evaluation:** Provides a deep dive into the itemized listing of controls, including testing conducted and test results.
- **Management response:** Notes exceptions and provides a response detailing how the organization plans to manage exceptions.

What's included in the Trust Services Criteria?

In a SOC 2 report, the Security Trust Services Criteria is always applicable, but most SOC 2 reports include just one or two additional criteria.

- **Security:** Controls to protect against unauthorized access, disclosure of information, and damage to systems. Seeks to understand whether the company has a security framework in place and controls over logical and physical access.

- **Confidentiality:** Controls to identify, manage, and dispose of / destroy confidential information (not personal information).

- **Processing Integrity:** Controls to ensure that system processing is accurate, timely and valid.

- **Availability:** Controls to ensure information and systems are made available and accessible at all times.

- **Privacy:** Controls to protect personally identifiable information (PII).

Why use a SOC 2 report?

Companies use SOC 2 reports when they:

- Are unwilling or unable to complete comprehensive IT controls assessments, such as for NIST or ISO, for themselves but still have to demonstrate control effectiveness
- Use a standard that is well-understood and comprehensive
- Have the flexibility to focus on a complete set of controls or just a subset

How do you interpret risks in a SOC 2 report?

A typical SOC 2 report will identify risks as “test results.” A typical SOC 2 Exceptions table looks like this:

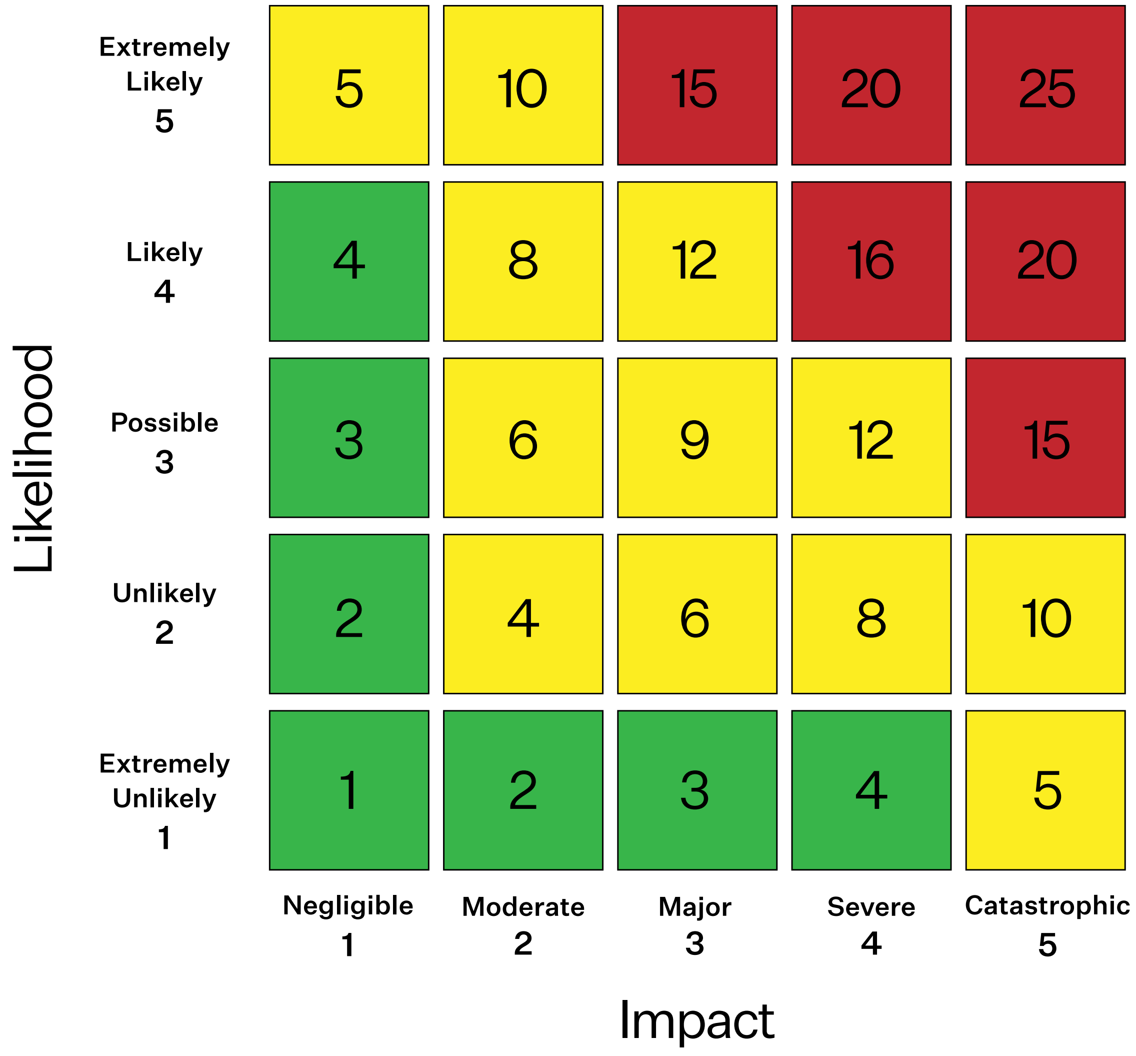
Control #	Criteria	Control Activity Specified by the Service Organization	Test of Operating Effectiveness	Test Results
CC 3.4	The Company identifies and assesses changes that could significantly impact the system of internal control.	Changes to the regulatory, economic, and physical environment in which the Company operates are considered and evaluated as part of the annual comprehensive risk assessment.	**Inspection:** Inspected the risk assessment worksheet and Risk Assessment Policy. Verification that changes to the regulatory, economic, and physical environment are considered and evaluated.	No exceptions noted.
		Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	**Inspection:** Inspected the risk assessment worksheet and Risk Assessment Policy. Verification that changes to the business structure and operations are considered and evaluated.	Lack of visibility for identifying business structure and operational change as part of the annual risk assessment.

- **Control #** is a code for tracking each control throughout its lifecycle.
- **Criteria** are descriptions of the controls as tested.
- **Control activity** explains how the company currently addresses that control.
- **Test of operating effectiveness** explains how the auditor inspected the control and what procedures were followed.
- **Test results** specify if there was an exception and what the deviation was.

There is no grading of risks in a SOC 2 report, such as red/amber/green indicators of risk failures.

This is where a third-party risk management platform can help!

How do you map SOC 2 control exceptions so you can centrally manage associated risks?



Likelihood					
Extremely Likely 5	🟨 5	🟨 10	🟥 15	🟥 20	🟥 25
Likely 4	🟩 4	🟨 8	🟨 12	🟥 16	🟥 20
Possible 3	🟩 3	🟨 6	🟨 9	🟨 12	🟥 15
Unlikely 2	🟩 2	🟨 4	🟨 6	🟨 8	🟨 10
Extremely Unlikely 1	🟩 1	🟩 2	🟩 3	🟩 4	🟨 5
	Negligible 1	Moderate 2	Major 3	Severe 4	Catastrophic 5
			Impact		

Translating SOC 2 control exceptions or test results to risks can be tricky without a way to centrally track third-party risks.

We recommending applying a “likelihood and impact” methodology to assign risk scores to any identified exceptions.

- **Likelihood** estimates the probability of a third party’s control failure impacting your organization’s operations.
- **Impact** estimates the level of disruption a control failure would have on your organization’s operations.

Using simple 0 to 5 scale, where 0 means no likelihood or impact and 5 means high likelihood or impact, you can create a heat map to quickly score and categorize risks.

Once risks are categorized into the heat map, you can define risk ownership, assign tasks, and engage with the third party for risk treatment and remediation.*

**Remember that the third party may have already addressed findings in the SOC 2 report Management Response section.*

What are the right key performance indicators (KPIs) and key risk indicators (KRIs) for SOC 2?

Risk and performance indicators help organizations to understand and track exposure to third-party risks and gain visibility over how well the TPRM program is performing. KPIs and KRIs should provide insights that measure:

- Risk compliance across the third-party ecosystem
- Common trends in critical risk areas
- Success rates in meeting TPRM goals
- Long-term trends in risk reduction (e.g., maturity)

… and be applicable to stakeholders including the Board and executive management, business owners, and procurement and security teams.

Below are a few standard KPIs and KRIs to consider as you evaluate risks across your third-party ecosystem. For more on KPIs and KRIs, check out our eBook, The 25 Most Important KPIs and KRIs for Third-Party Risk Management.

Key Risk Indicators	Key Performance Indicators
Objective: Identify the level of exposure to risk	**Objective: Measure the performance of the third-party risk management program**
• Number of high-risk vendors based on overall security posture	• Percentage of completed vendor assessments
• Areas of risk within critical controls or control groups	• Percentage reduction in overall risk scores for each vendor
• Financial, reputational, or operational changes that increase business exposure	• Number of vendors with high compliance ratings against industry standards and other baselines

How can you simplify the process of tracking and remediating SOC 2 risks?

Start by developing a playbook for remediating SOC 2 exceptions based on:

- **Minimum/mandatory requirements:** Identify what is absolutely required of third parties. If there is an exception in an area, then the third party is compelled to remediate it.
- **Best practices:** Incorporate your firm's expectation of how a risk or control exception should be remediated based on industry best practices.
- **Timelines:** Set timeframes based on the severity of risks.
- **Decisions or resulting actions:** Define what happens to remediated risks. Will you accept the remediation and lower the risk score based on your firm's risk appetite, or will you close down the risk with no further action required?

Clearly state the requirement. If you expect further evidence, then specify when you need it. Also, confirm whether you require ongoing monitoring or remediation.

Leverage existing risk registers to map these control exceptions into what you already have. This approach helps you cross-map findings for compliance reporting against other frameworks.

Managing third-party risks – regardless of whether or not they were discovered via a SOC 2 report – is impossible without a central platform that automates risk identification, assessment, triage, monitoring and remediation. That's where Prevalent™ can help!

Getting Started with SOC 2 Third-Party Risk Management

Prevalent can help simplify SOC 2 third-party risk management using solutions and professionals with SOC 2 subject matter expertise. Prevalent SOC 2 Exception Analysis Services:

- Review complete SOC 2 reports and conduct a brief contextual interview with the business owner
- Provide a summary report on findings and recommendations based on the scope of services, the SOC 2 report, and each domain area in a consistent, easy-to-consume format
- Identify any missing control criteria considered appropriate based on the service provided
- Advise on suitability of the SOC 2 against the service provided, and provide guidance on any remedial actions
- Map SOC 2 control criteria to common industry frameworks such as the SIG Lite or the Prevalent Compliance Framework (PCF)

Ready to get started?

For more on Prevalent's SOC 2 Exception Analysis Services, download the data sheet or contact us for a strategy discussion today!

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors and suppliers througout the third-party lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

Visit www.prevalent.net to learn more.