SOC report review checklist

A SOC report on file proves little until someone has read it. Most of what matters sits in a few places. This checklist walks through them in the order they appear in a typical report and ends with the conclusion you should write down.

Vendor _____ Completed by _____ Date _____

Confirm you have the right report

- [ ] The report is the type your policy asks for. A Type II report tests controls over a period. A Type I report describes them at a single date.
- [ ] The period covered is recent, and it follows on from the last report you hold without a gap.
- [ ] A bridge letter covers the time between the end of the period and today, if that is more than a few months.
- [ ] The report was issued by an independent audit firm.
- [ ] The system described is the product or service you use, at the locations that serve you.

Read the auditor's opinion

- [ ] The opinion is unqualified. A qualified or adverse opinion, or a disclaimer, needs a written follow-up with the vendor.
- [ ] Any qualification is read in full, and you understand which controls it concerns.
- [ ] Management's assertion matches the scope you expected.

Check the scope

- [ ] The services, applications and data centers you depend on are inside the scope.
- [ ] The criteria covered are the ones you need, such as security, availability and confidentiality.
- [ ] Anything you rely on that is outside the scope is noted, with how you will get assurance on it.

Look at subservice organizations

Most vendors rely on others, such as a cloud hosting provider. The report says how they were treated.

- [ ] Every subservice organization is listed, with what it does for the vendor.
- [ ] You know whether each one was included in the testing or carved out of it.
- [ ] For a carved-out provider that matters to you, you have its own report or the vendor's account of how it monitors that provider.

Map the user controls to your own

The report lists controls the vendor expects you to operate. If you do not operate them, the vendor's controls may not protect you.

- [ ] Every complementary user control is listed against the person or team at your institution who performs it.
- [ ] Controls you do not perform today are recorded as gaps with an owner and a due date.

Review the test results

- [ ] Every exception is read, including the ones the auditor considered minor.
- [ ] Management's response to each exception says what was fixed and when.
- [ ] Exceptions that repeat from the previous report are followed up with the vendor.
- [ ] You have judged whether any exception affects the services or data you care about.

Write down the conclusion

- [ ] A short written summary records who reviewed the report, when, and what they concluded.
- [ ] Open questions are sent to the vendor and tracked to an answer.
- [ ] Gaps and exceptions that need action become remediation items.
- [ ] The report's expiration date is recorded, so the next one is requested on time.

What the auditor's opinion means

Opinion	What it tells you	What to do
Unqualified	The controls were described fairly and worked as intended	Continue with the rest of the review
Qualified	The auditor found a problem with specific controls	Read the qualification and ask the vendor what has changed
Adverse	The controls were not suitably designed or did not work	Escalate and reconsider the vendor's risk level
Disclaimer	The auditor could not gather enough evidence to give an opinion	Treat the report as no assurance and escalate

A free checklist from VendorRisk, vendor management software for regulated institutions. More guides, checklists and templates at vendorrisk.com/resources.