ZenGRC

Preparing for a SOC 2 or SOC 3 audit

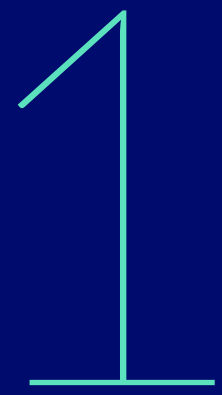
Three easy steps

Getting certified as compliant with Service Organization Controls (SOC) 2 or SOC 3 is one of the best actions you can take to assure customers and clients that you care about their privacy.

And in fact, this certification has become a deal-breaker for many: if you aren't SOC certified, they will not do business with you.

Established by the American Institute of Certified Public Accountants (AICPA), SOC 2/3, a voluntary regulatory framework, assesses non-financial reporting controls on how organizations and their service providers process, store, and secure data. It's all about information security and privacy.

Passing a SOC 2/3 audit—be it a yearly or even a one-time assessment of your policies, procedures, and practices—attests that you are committed to handling sensitive information with care.



Establish your goals

Audits for SOC 2 and SOC 3 cover the same areas, which is why we address them together in this book. The difference between the two lies in the detail and specificity of the audit report. Which is right for your organization?

As you begin collecting and organizing documents for your SOC 2/3 audit, you'll need to determine not only which framework suits your purposes, but also the audit type and its scope.

Start by asking yourself why you are conducting the audit.

Do you want certification regarding a particular product or service, or for your entire organization? What do you need the report to say? You may want to engage your auditor in a discussion about these questions, including:

What type of audit do you want?

- Type 1 audits examine your controls at a point in time.
- Type 2 tests your controls' effectiveness over an entire year.

Many organizations start with Type 1 to set a baseline, then follow up with Type 2 audits conducted annually.

Who is the report intended for?

- SOC 2 audit reports provide information about your enterprise to an informed, knowledgeable audience whose members often have a vested interest in the audit findings.
- SOC 3 reports address a more general audience, and tend to be shorter and less detailed than SOC 2 audits.

What will be the scope of your audit?

SOC 2/3 comprises 61 Trust Services Criteria, but you will most likely not be audited against them all. Which of the criteria pertain to your organization?

2 Organize your materials

Once you have determined the scope and nature of your SOC 2 or SOC 3 audit, you will need to consider the Trust Services Criteria that you and your auditor have selected. For each, you should determine which of your enterprise's controls apply and whether they are effective, resolve any gaps, and gather the documents you need as proof.

ORGANIZE YOUR MATERIALS IN LINE WITH THE FIVE OVERARCHING SOC 2/3 TRUST SERVICES PRINCIPLES:

Security.

This principle refers to the controls your enterprise uses to protect the security of personal, proprietary, and confidential information. Questions include:

- ☐ How secure are your buildings? Do you secure your processing facilities including office spaces to ensure that only authorized personnel can gain access to them?
- ☐ Do you have logical controls on virtual access including user logins before each instance and restricted access on a need-to-use basis?
- ☐ Do you have controls on data transmission? Do you have firewalls in place to prevent unauthorized access? Do you encrypt transmitted and stored data?

Availability.

For a business to run smoothly in this day and age, its computer systems and networks must operate around the clock. Ecommerce and cybersecurity both rely on systems' being operational.

- ☐ Do you have controls in place to ensure that your systems are available when you need them to be? What are those controls?
- ☐ Do you monitor capacity to avoid overloads? How?
- ☐ Do you have disaster recovery procedures in place? What are they?

Confidentiality.

Certain types of data merit special protection: Personally Identifiable Information (PII) such as Social Security number, date of birth, and mother's maiden name; credit card numbers, and medical and health information.

- ☐ Have you tagged or otherwise identified these data types?
- ☐ Do you know where these sensitive forms of data are being processed and stored, how they are processed, and why?

If you are governed by the GDPR, PCI, or HIPAA, you should have ready access to this information.

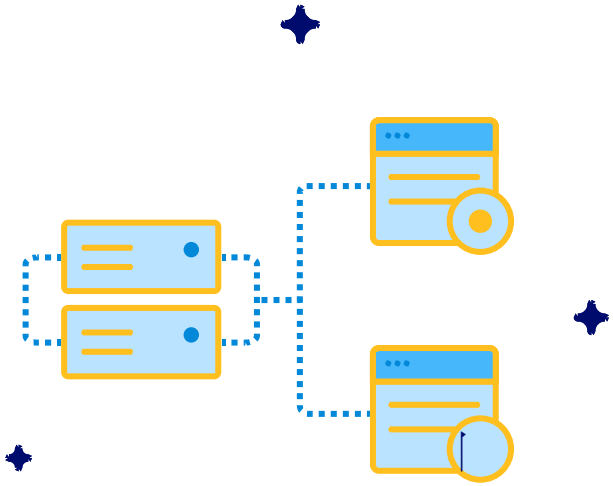
Processing integrity.

Processed data often includes errors. Whether it's a birthdate erroneously recorded; credit card numbers transposed; a name spelled incorrectly, or something else, bad data can harm not only your clients, customers, and patients, but also your organization. SOC 2/3 holds your enterprise accountable for maintaining the accuracy of the data it collects.

For instance, if you are a service provider—such as a cloud provider—and you are aggregating data from multiple points, it is important to know where data is coming from and how reliable your sources are, and to feel confident that your own people and processes are not altering it. Otherwise, you could be providing false or faulty information.

Likewise, if your firm provides financial management, accounting services, or ecommerce, good data is essential to providing the best services possible—and could make the difference between profits and loss.

- What mechanisms do you have in place for double-checking the data in your system to ensure that it is correct?
- What kinds of data are you processing? Who are you processing data for?
- If you're a service user, what data are you sending out for processing, who are you sending it to, and what are they doing with it?



Oftentimes, companies create data-flow diagrams to show where they are getting data, how it is being processed, and the output—where it is going or how it is being consumed.

Privacy.

In recent years, privacy has become closely linked to security, and with good reason: in stealing our information, data thieves also rob us of our identities. In a SOC audit, privacy refers specifically to measures an enterprise takes to protect personal, proprietary, and sensitive data for authorized eyes only.

- ☐ How do you ensure that data you collect about someone is only used for the purposes you have stated?
- ☐ How do you restrict data access to those who need it to do their jobs?
- ☐ How do you protect the identity of data owners? Do you change data to mask its owners' identity ("pseudonymization") or remove identifying data altogether ("anonymization")?
- ☐ Are you able to remove data from your systems and networks if asked?
- ☐ How do you dispose of data to ensure that it does not fall into unauthorized hands?

You will need evidence to back up every answer to these and other questions your auditor might pose. Most commonly, you will provide "expected artifacts," such as policies and procedures documents, fraud protection statements, and data-flow charts. Other types of evidence include contracts, emails, and screenshots. In each case, you will want to confirm with your auditor that the artifact you are providing is sufficient.

3 Examine yourself

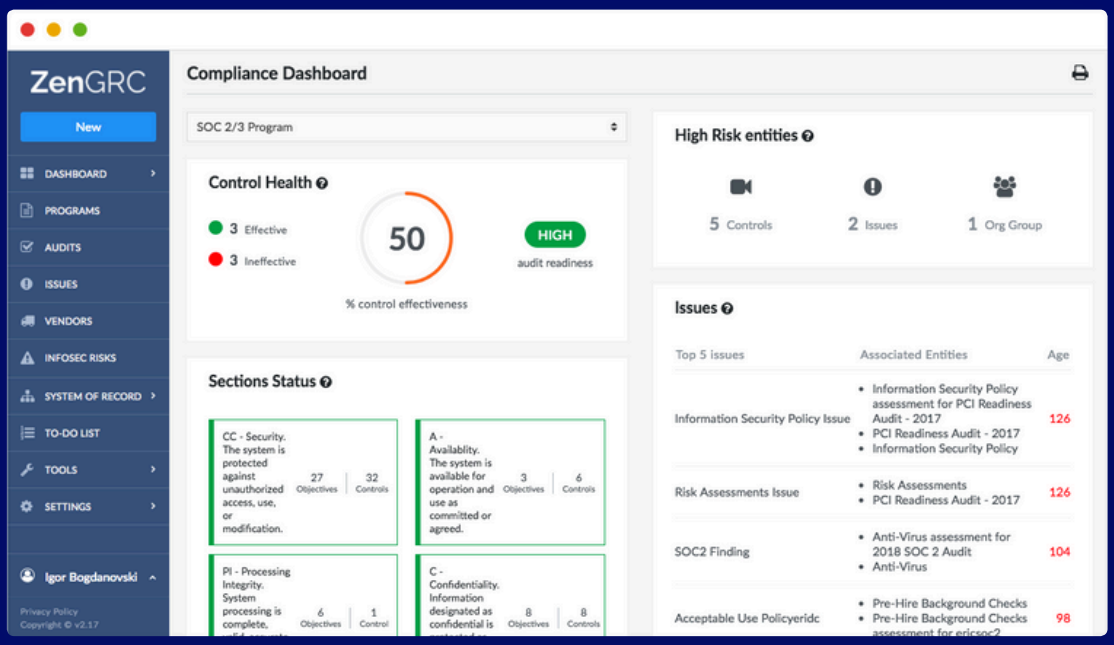
The key to a relatively-hassle-free SOC 2/3 audit lies in the advance work. If you wait until the last moment to pull together documentation and identify and fill gaps, you may face audit findings and a denial of certification—more harmful than if you had not sought certification in the first place.

Most organizations, however, have come to expect SOC 2/3 certification from those they do business with—meaning that getting that "seal of approval" is a must.

To make SOC 2/3 certification easier on your enterprise and people as well as the auditor, peruse your systems and policies well in advance, and take steps to resolve any issues you might find. Just having a plan to put needed controls into place can go a long way toward satisfying an auditor's concerns.

Get help if you need it

Continually monitoring your enterprise's and service providers' systems, networks, and procedures can be a big task even for the smallest business. Periodic self-audits by an internal or outsourced auditor, or using a quality governance, risk and compliance (GRC) software, can really take the pressure off at SOC 2/3 audit time.



With proper preparation, you should be able to pass the SOC 2/3 test with flying colors after minimal effort. That coveted certification in hand, you then will be freed to focus your time and energies on the business at hand: serving your customers and clients, and boosting your bottom line.

The Checklist

1. ESTABLISH YOUR GOALS

What type of audit do you want?

- ◯ Type 1 audits examine your controls at a point in time.
- ◯ Type 2 tests your controls' effectiveness over an entire year.

Who is the report intended for?

- ◯ SOC 2 audit reports provide information about your enterprise to an informed, knowledgeable audience whose members often have a vested interest in the audit findings.
- ◯ SOC 3 reports address a more general audience, and tend to be shorter and less detailed than SOC 2 audits.

2. ORGANIZE YOUR MATERIALS

Security.

- ◯ How secure are your buildings? Do you secure your processing facilities including office spaces to ensure that only authorized personnel can gain access to them?
- ◯ Do you have logical controls on virtual access including user logins before each instance and restricted access on a need-to-use basis?
- ◯ Do you have controls on data transmission? Do you have firewalls in place to prevent unauthorized access? Do you encrypt transmitted and stored data?

Availability.

- ◯ Do you have controls in place to ensure that your systems are available when you need them to be? What are those controls?
- ◯ Do you monitor capacity to avoid overloads? How?
- ◯ Do you have disaster recovery procedures in place? What are they?

Confidentiality.

- ◯ Have you tagged or otherwise identified these data types?
- ◯ Do you know where these sensitive forms of data are being processed and stored, how they are processed, and why?

Processing integrity.

- ◯ What mechanisms do you have in place for double-checking the data in your system to ensure that it is correct?
- ◯ What kinds of data are you processing? Who are you processing data for?
- ◯ If you're a service user, what data are you sending out for processing, who are you sending it to, and what are they doing with it?

Privacy.

- ◯ How do you ensure that data you collect about someone is only used for the purposes you have stated?
- ◯ How do you restrict data access to those who need it to do their jobs?
- ◯ How do you protect the identity of data owners? Do you change data to mask its owners' identity ("pseudonymization") or remove identifying data altogether ("anonymization")?
- ◯ Are you able to remove data from your systems and networks if asked?
- ◯ How do you dispose of data to ensure that it does not fall into unauthorized hands?

About ZenGRC

ZenGRC helps streamline the world's leading company's GRC needs. Our cloud-based solution with fast, easy deployment, unified controls management, and a centralized dashboard offers simple, streamlined compliance and risk management, including self-audits, without the hassle and confusion of spreadsheets. Contact a ZenGRC expert today to request your free demo, and embark on the worry-free path to regulatory compliance—the Zen way.

www.ZenGRC.com/resources
engage@ZenGRC.com
(877) 440-7971