How to build trust and security through SOC 2 reporting?

SOC 2 - A Foundation for Trust, Security, and Operational Excellence when managing customer data

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Why SOC 2 Matters

In today’s digital economy, organizations face increasing pressure to demonstrate that they can protect sensitive data, maintain system integrity, and operate securely. SOC 2 is one of the most widely recognized frameworks for achieving this type of assurance.

Developed by the American Institute of **Certified Public Accountants (AICPA)**, SOC 2 (System and Organization Controls to securely manage customer data) provides a compliance framework for evaluating how service organizations manage data across five **Trust Services Criteria (TSC)**:

- **Security (Common) Criteria**: Protection against unauthorized access and system vulnerabilities.
- **Availability**: Ensuring systems are operational and accessible as promised.
- **Processing Integrity**: Ensuring systems process data accurately and reliably.
- **Confidentiality**: Safeguarding sensitive business information.
- **Privacy**: Protecting personal data in accordance with privacy principles.

SOC 2 is not a checklist– it offers a flexible, risk-based framework that allows organizations to design controls tailored to their operations, while still meeting industry expectations for security and governance.

Importance of SOC 2 for your business

SOC 2 compliance gives your business and clients confidence in security, quality, and compliance. It helps you:

- Build trust with clients, partners, and regulators
- Prove service integrity and operational maturity
- Speed up sales and simplify audits
- Align with GDPR, HIPAA, DORA and other regulátory and industry frameworks
- Support responsible AI and scalable growth

With SOC 2, you remove barriers, reduce risk, and unlock enterprise opportunities – all while giving your clients peace of mind. Compared to ISO27K certification, SOC 2 is recognized globally, providing a competitive edge in the marketplace by demonstrating your commitment to data security and operational excellence. Additionally, its broader scope encompasses not only security but also availability, processing integrity, confidentiality, and privacy, allowing you to address a wider range of client concerns and enhance trust across diverse industries.

What EY can offer

EY provides a wide suite of services to support your SOC 2 journey and broader assurance needs. All of these are described in the following pages.

How to start your SOC 2 reporting journey

- Readiness assessment for SOC 2
- Issuance of SOC 2 Reports: Type 1 & Type 2

Meet your reporting needs with SOC 2

- Addressing DORA Requirements with SOC 2
- ISAE 3000 vs SSAE18 standards
- Assurance over AI Governance

SOC 2+ & SOC 3

- SOC 2+: Extending Assurance
- SOC 3: Share Your Security Commitment with the Public

How to start your SOC 2 reporting journey

Conduct a readiness assessment for SOC 2

Pursuing a SOC 2 report is not just a compliance milestone – it is a signal of organizational maturity. Through SOC 2, companies can demonstrate:

- A structured approach to risk management and internal controls
- A commitment to transparency and accountability
- The ability to scale securely while maintaining trust with clients and partners

Typically, organizations ready for SOC 2 have already implemented foundational security practices such as access control, incident response, change management, and vendor oversight.

Whether you are a startup preparing to enter regulated markets or an enterprise expanding globally, SOC 2 is a strategic investment in your long-term credibility and operational resilience.

To support your first steps in the SOC 2 reporting journey and assure you that your organization is ready for it, EY offers a **Readiness Assessment**. The Readiness Assessment, typically lasting 6 – 8 weeks, helps organizations evaluate the maturity of their control environment, identify gaps, and prepare effectively for their first SOC 2 report.

Prepare for issuance of SOC 2 reports: Type 1 and Type 2

We offer both SOC 2 Type 1 and SOC 2 Type 2 reports:

- **Type 1** evaluates the design of controls at a specific point in time. It answers the question: *Are the controls properly designed to meet the selected criteria?*
- **Type 2** assesses the operational effectiveness of those controls over a defined period (typically 3–12 months). It answers: *Do the controls function as intended over a period of time?*

Clients often begin with a Type 1 report to establish a baseline, then progress to Type 2 for deeper assurance. We support both paths and tailor reporting to meet the needs of startups, enterprises, and regulated industries.

Meet your reporting needs with SOC 2

Addressing DORA Requirements with SOC 2

The **Digital Operational Resilience Act (DORA)** is a European regulation aimed at strengthening the ICT risk management and operational resilience of financial entities and their service providers.

SOC 2 is increasingly recognized as a suitable framework for addressing DORA requirements, especially for ICT service providers. It offers a structured and independently audited approach to demonstrating compliance with key DORA principles.

As **SOC 2** provides a more detailed and flexible assurance report based on the effectiveness of specific controls over time, this makes SOC 2 particularly valuable for demonstrating alignment with DORA's expectations around the following key areas:

ICT Risk Management: SOC 2 Security (Common) Criteria cover risk identification, assessment, mitigation, and monitoring—core pillars of DORA.

Incident Response and Reporting: System operations and monitoring controls support timely detection and reporting of ICT disruptions.

Third-Party Risk Oversight: SOC 2 includes controls for managing subservice organizations and vendors, aligning with DORA's outsourcing requirements.

Business Continuity and Recovery: Availability and Security (Common) Criteria ensure alignment with DORA's expectations for continuity planning and disaster recovery.

ISAE 3000 vs SSAE18 standards

When it comes to demonstrating trust, security, and control, choosing the right assurance standard matters. We offer **SOC 2** reports under both **SSAE 18** and **ISAE 3000**, giving you flexibility to meet client expectations across markets.

- **SSAE 18** is the U.S. standard that underpins SOC 2 reporting. It is widely recognized and ideal for organizations operating primarily in North America.
- **ISAE 3000** is an international standard for non-financial assurance. It allows for broader, more customized reporting—perfect for global businesses and emerging areas like ESG and AI governance.

While **SOC 2 can be issued under ISAE 3000**, the ISAE 3000 framework also allows us to go beyond the scope of SOC 2. This means we can tailor assurance reports to your specific demands—whether you are looking to validate internal controls, demonstrate ethical AI practices, or meet unique regulatory requirements.

SOC 2 Assurance over AI Governance

We offer assurance over **AI governance** under both SOC 2 and ISAE 3000 depending on your IT landscape and individual needs. This way, we can help your organization establish trust in how AI systems are designed, deployed and monitored. Whether you are looking to validate data handling, algorithmic transparency or ethical oversight, we provide assurance that supports responsible innovation and regulatory alignment.

SOC 2+ & SOC 3

EY's Credentials in SOC 2 Auditing

Ernst & Young (EY) is a global market leader in SOC reporting, issuing over 3 750 SOC reports annually for more than 2 600 clients. With deep expertise across industries—including technology, healthcare, finance, and asset management—EY supports organizations in achieving robust compliance and operational assurance. SOC 2 audits help clients build trust, reduce audit fatigue, and demonstrate security maturity to stakeholders.

SOC 2+: Extending Assurance

SOC 2+ enhances the value of a standard SOC 2 report by mapping its controls to additional internationally recognized frameworks. This approach helps organizations demonstrate broader compliance and meet expectations across multiple jurisdictions and industries.

SOC 2+ can incorporate criteria defined by regulatory and industry frameworks such as:

- ISO/IEC 27001: Information Security Management System (ISMS)
- GDPR: European data protection and privacy regulation
- HIPAA: Health Insurance Portability and Accountability Act –law that protects patient privacy and secures health information
- HITRUST: Health Information Trust Alliance Common Security Framework
- CSA STAR: Cloud Security Alliance Framework
- DORA: Digital Operational Resilience Act (EU)

This mapping helps ensure that SOC 2 controls are not only effective but also globally relevant, helping clients meet cross-border compliance requirements and industry-specific expectations.

SOC 3: Share Your Security Commitment with the Public

Unlike SOC 2, which is detailed and confidential, SOC 3 is a public-facing summary of the same controls. It is designed for broad distribution and can be published on a company’s website or shared with stakeholders without the need for NDAs.

SOC 3 helps you communicate your commitment to security and other criteria in a manner accessible to a wider audience.

Ready to strengthen your operational resilience?

Let's start the conversation.

Josef Duben

Senior Manager

+420 731 642 752

josef.duben@cz.ey.com

Milada Závodová

Senior Manager

+420 603 577 830

milada.zavodova@cz.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.cz.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.cz