Are you measuring everything you need to build trust?

System and Organization Controls (SOC)
SOC 2 – SOC for Service Organizations: Trust Services Criteria

March 2021

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

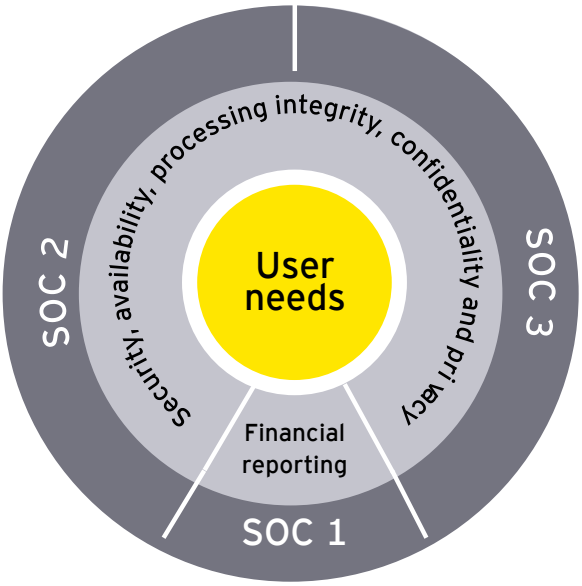
EY
Building a better working world

Demystifying SOC 2

SOC Reporting types

- SOC 1 provides information about controls at a service organization relevant to a user entity's internal control over financial reporting (restricted use).
- SOC 2 provides information about the effectiveness of controls that help achieve the service organization's service commitments and system requirements, based on the applicable trust services criteria related to security, availability, processing integrity, confidentiality or privacy (restricted use).
- SOC 3 does not provide as much information as SOC 2. SOC 3 works similar to SOC 2, however, it has different reporting requirements (general use).

Which SOC report is right for you?



Instilling trust through SOC Reporting

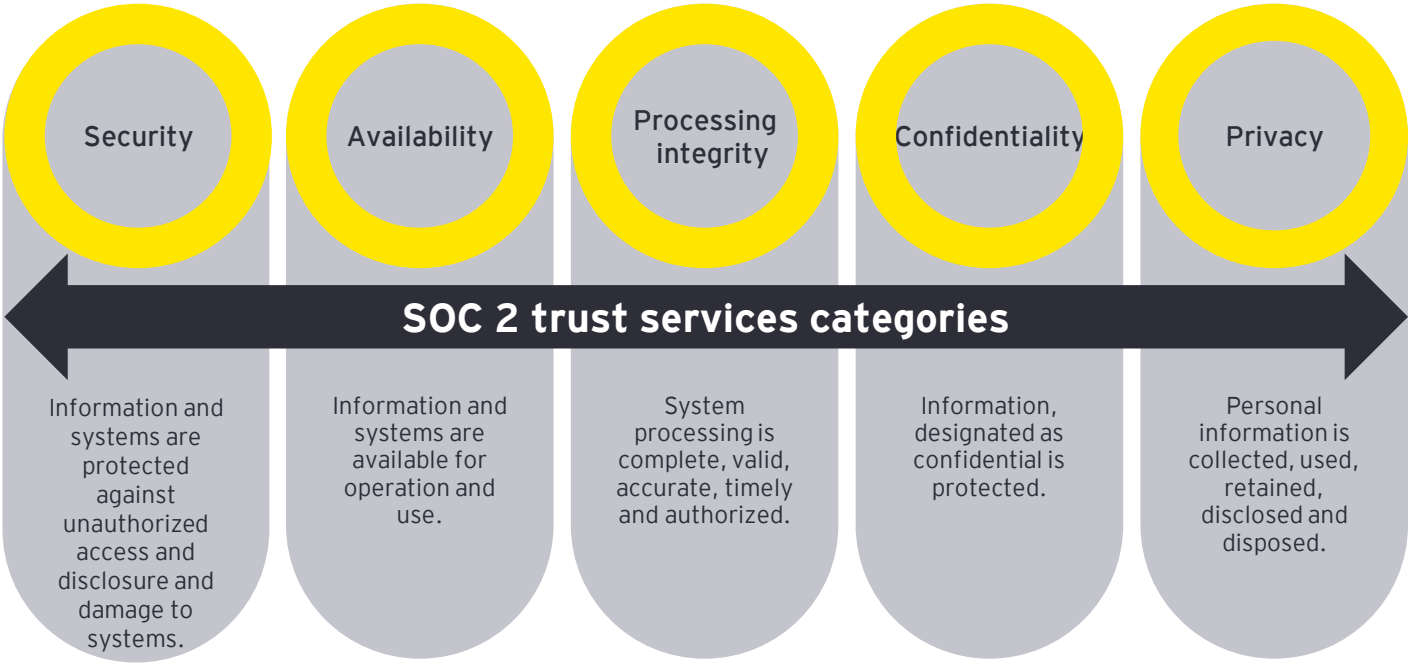
SOC reporting is about instilling trust. Trust is earned by the service organization by delivering against what was promised, transparency about its operations and risk management, and independent audit. It's a delicate balance between promise, execution and the communication on execution. SOC reporting, therefore, provides value to your clients. In many cases, your clients use SOC reports help demonstrate their compliance to regulator and supervisory body requirements.

Improve stakeholder communications with SOC 2 report

SOC 2 reports build trust with your stakeholders and allow you to identify areas for improvement. They are used to understand a service organization's internal controls related to criteria such as confidentiality, availability, processing integrity (the conventional information security triangle), security and privacy.

SOC 2 - SOC for Service Organizations: Trust Services Criteria

Where SOC 1 reports provide assurance to only financially significant processes, SOC 2 reports can provide assurance over nonfinancially related processes. SOC 2 reports provide assurance in relation to one or more of the five trust services categories to help meet the entity's objectives, which are:



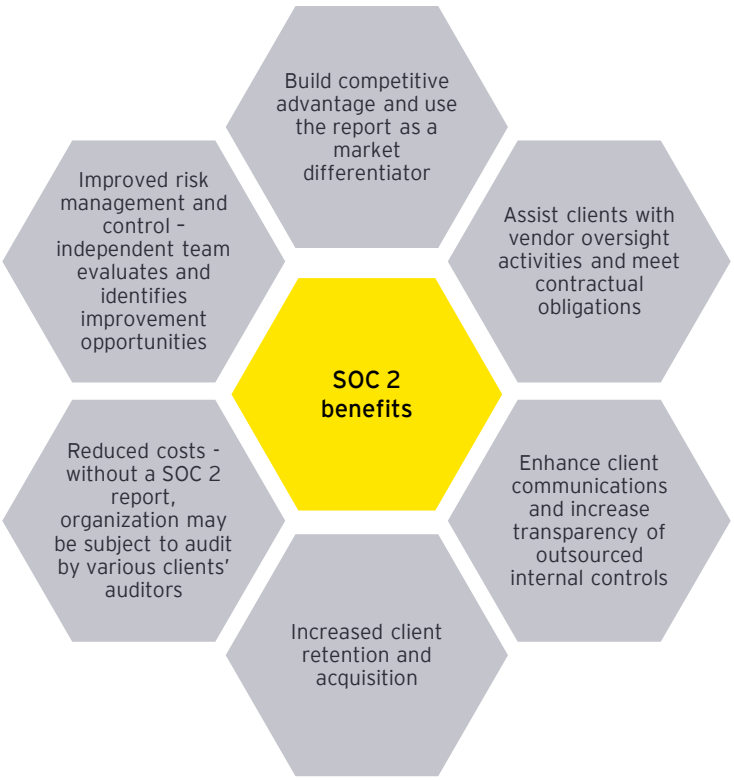
A streamlined approach to help deliver SOC 2 report to your clients

SOC 2 reports can be tailored to meet the needs of specific industries. The trust services criteria used in SOC 2 reports have been mapped to various other standards. As a result of this mapping, the SOC 2 testing can be used to support other certifications, helping achieve a streamlined approach to testing. The mapping allows one set of testing to provide assurance against multiple standards. Examples of service organizations that could benefit from a SOC 2 include:

- Data center hosting provider reporting on security and availability
- Cloud service providers reporting on processing integrity, security and availability (in accordance with Cloud Security Alliance standards)
- Health care provider, reporting on compliance [e.g., Health Insurance Portability and Accountability Act (HIPAA) or Health Information Trust Alliance (HITRUST)]
- Credit card processors or payment service providers, reporting on processing integrity and data confidentiality [similar to Payment Card Industry Data Security Standard (PCI DSS)]
- Application service provider outsourcer, reporting on security and availability
- Companies providing Blockchain-as-a-Service (BaaS) or using emerging technologies, such as blockchain and artificial intelligence to provide services to its customers
- Background verification companies or identity verification service providers reporting on security, confidentiality, processing integrity and privacy

SOC 2 benefits

SOC 2 is an opportunity to provide assurance on a wider range of service provision than just financial reporting. Some of the benefits include:



Additionally, SOC 2+ ("SOC 2 Plus") report can incorporate a service auditor's opinion on additional subject matter or a mapping to established reporting frameworks, providing greater reporting flexibility and customer satisfaction. Reporting frameworks such as ISO 27001, General Data Protection Regulation (GDPR), Cloud Controls Matrix, National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), HIPAA and HITRUST can be used together with SOC 2 reports.

Newer reporting options, such as SOC for Supply Chain, SOC for Cybersecurity and Data Integrity, help provide greater trust to internal and external stakeholders.

The EY SOC 2 approach and methodology

Develop expectations	Plan SOC 2 examination	Perform examination	Report results
User organization: ► Regulatory ► Audit requirements	Understand the key business processes and user organization needs and expectations	► Evaluate risk assessment ► Evaluate system design and perform test of operating effectiveness	External communication SOC 2 report as of, or for a specified period
Service organization: ► Regulatory ► Audit requirements	Plan and scope the engagement	Review results with management	
Service expectations and relationship protocols	Develop detailed testing approach and work programme	Summarize executive management and audit committee communications	► Internal communication ► Management letter

Repeat at subsequent periods using lessons learned

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

About EY SOC Reporting
The EY organization plays an important role internationally in the SOC reporting landscape. We have representatives in working groups defining the professional standards that are used for SOC reporting. We have professionals worldwide whose daily work is providing SOC reports to EY clients. All this leads to a substantial amount of thought leadership on SOC reporting within our organization. Thought leadership is available through EY professionals that work together on a daily basis to develop an effective and efficient SOC reporting process for our clients.

EYG no. 002176-21Gbl
ED None

ey.com

Chris Halterman
Managing Director, Business Consulting
chris.halterman@ey.com
Global SOC Reporting Leader
Ernst & Young LLP

Dennis Houtekamer
Associate Partner, Technology Risk
dennis.houtekamer@nl.ey.com
EMEIA SOC Reporting Leader
Ernst & Young Accountants LLP