SECURANCE

# Step-by-step Guide - **SOC 2 Compliance.**

# SOC 2 Compliance

## Outsourcing | Trust Services Criteria

**SOC 2 is a Service Organization Control (SOC) report which provides assurance over outsourced processes. An audit performed in accordance with SOC 2 is widely recognized, because it represents an in-depth audit of a service organization's control activities, which include controls over internal control, security, risk management, and related processes. SOC 2 reports are drafted in accordance with the Trust Services Criteria.**

**SOC 2 focuses on a business' non-financial reporting controls as they relate to Security, Availability, Processing integrity, Confidentiality, and Privacy. These principles are outlines in the Trust Services Criteria. Each of the criteria has defined requirements (Points of Focus) which serve as a guidance to demonstrate adherence to the criteria.**

### Modular

SOC 2 reports are modular, implying that reports can cover one or more of the principles, depending on the needs and requirements of a service organisation. The only criteria that are mandatory for SOC 2 are the security criteria. These criteria are also referred to as the common criteria.

### Common Criteria

The only criteria that are mandatory for SOC 2 is Security, which are also referred to as the Common Criteria, Additional criteria can be included within the scope of a SOC 2 reporting.

In addition to security requirements (Logical and Physical Access Controls, System Operations, and Change Management), the Common Criteria also contain requirements for an internal control framework, including risk management (COSO). The key elements of the COSO framework are Control Environment, Communication and Information, Risk Assessment and Risk Mitigation, Monitoring Activities and Control Activities.

The chosen criteria are implemented within the organisation and outlined in the SOC 2 report by following the points of focus and additional criteria as outlined in the COSO 2013 (risk management) framework and the Trust Services Criteria. Hereafter the SOC 2 report is audited by independent audit firms.

# Trust Services Criteria

## Criteria Explained

**The only mandatory criteria are the Security criteria, as previously outlined. More often, the applicability of the Availability, Confidentiality, Processing Integrity, and Privacy criteria are considered based on the services provided, and in conjunction with key clients and SOC 2 experts. When an organization chooses to include criteria, all associated requirements and points of focus must be considered and implemented when applicable. Key characteristics per criteria are outlined below.**

### SECURITY

Security refers to the protection of data throughout its life cycle. Security controls are put in place to protect against unauthorised disclosure, unauthorised access or damage to systems that could affect other criteria.

### AVAILABILITY

Availability refers to controls that demonstrate that systems remain operational and perform to meet established business objectives and service level agreements.

### CONFIDENTIALITY

Confidentiality requires companies to demonstrate their ability to safeguard confidential information throughout its lifecycle, including its collection, processing and disposal.

### PROCESSING INTEGRITY

Integrity of use must ensure that data is processed in a predictable manner, without unexplained or random errors.

### PRIVACY

Privacy is similar to Confidentiality, but has distinctive application to personally identifiable information (PII), especially information your organisation obtains from its customers.

# PHASE 1. SCOPE DEFINITION

## How to Define the Scope of a SOC 2 Report

**The scope of a SOC 2 report relates to the (non-financial) controls within a service organisation relevant to Security, Availability, Processing Integrity, Confidentiality and/or Privacy, which are defined in the Trust Service Criteria. The SOC 2 report should contain a scope section that notes the key components of the scope. It is required to include details about the type(s) of services provided and also the Infrastructure, Software, People, Policies and Procedures, and Data relevant to those services.**

### Example

For a Software as a Service (SaaS) provider their scope is typically their software application(s) accessible to their clients. This includes all the data held in it, the infrastructure that hosts it, and the people and procedures that support it. The sub-service providers and complementary user entity control areas give further details regarding the scope in other sections of the report by defining the boundaries of the scope within the report.

### Conclusion

In the end the scope of an SOC 2 report is up to management to define. The controls focused on the service organization's operations that are substantial to the organization's non-financial statements must be included in the scope. Besides the fact that the scope must be clearly defined and disclosed in the report, there is some flexibility. Eventually, the responsibility for ensuring the report meets the requirements of its end-users lies with management.

# Competitive Advantage

## How a SOC 2 Report Gives You an Edge Over Your Competitors

**SOC 2 provides a competitive advantage by distinguishing service organizations from their competitors. The advantages of SOC 2 reports encompass enhancing and fine-tuning risk management, while also fostering market confidence through transparent presentation of the control framework. The implementation of SOC 2 enhances audit efficiency and minimizes operational inefficiencies within the business.**

# PHASE 2. Implementation

## Step-by-step Approach


### 1. Impact Analysis & Planning

In Phase 1, the impact (GAP analysis) of the implementation for determined, and the applicability of the Trust Services Criteria is assessed. Based on the impact and the defined scope of the implementation, a detailed plan is prepared in which the various milestones are identified and arrangements with management are made

### 2. Processes & Controls

In Phase 2, interviews are held to identify risks, determine the impact and the existing working method, and take note of the information present within the organization. The organization control measures are then described according to the SOC 2 requirements based on the information obtained from the interviews. These are recorded in a control matrix; a matrix containing the SOC 2 requirements and related control measures. We will advise proactively on the implementation of any missing controls (including process descriptions).

### 3. Control Framework

In Phase 3, Securance will describe the control framework based on the most recent COSO framework (COSO 2013) and will prepare the general section of the reporting. In the general section a description of the processes, the organization and the General IT Controls is included.

### 4. SOC 2 Report

In Phase 4 the full SOC 2 report is prepared based on the individual sections and additional sections such as the management statement, and the complementary user entity controls. Phase 4 results in a draft SOC 2 report. We will discuss this report in detail with relevant staff. The organization will implement any identified missing controls within the organization during this phase.

*The processing time of the first four phases will be between six to eight weeks, depending on the commitment and availability of employees. The required availability of C-level executives is expected to be one day per week during that period.*

## 5. Pre-Audit

After the preparation of the report, Securance will carry out a pre-audit or 'walkthrough' in Phase 5. During the pre-audit the control measures will be tested, and possible problem areas will be identified prior to the final audit. During this phase, the organization will provide the documentation and evidence required by Securance.

## 6. Redressing

During Phase 6, as a result of the pre-audit, improvements in control measures and the management system are implemented and solutions are prepared for the identified problem areas. Securance will provide solutions that can be implemented within the organization and the SOC 2 report. Phase 6 will result in the final SOC 2 report.

*The processing time of Phases 5 and 6 is between two and four weeks. The required availability of employees is expected to be one day per week during that period.*

# PHASE 3. The Audit

## Quality Assurance Audits

### The SOC 2 Audits Explained

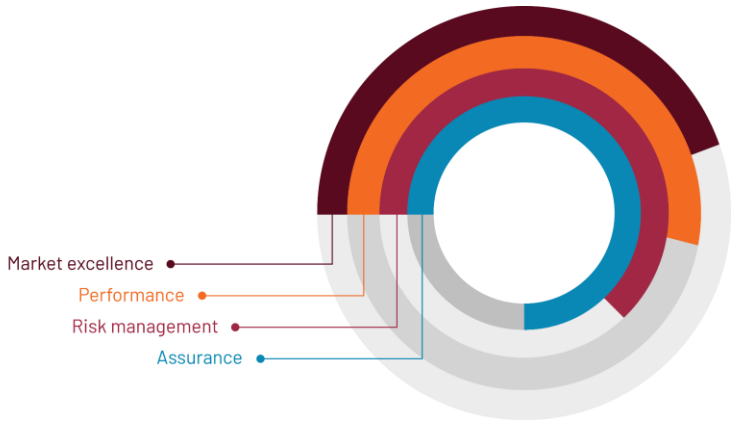
The key is to successful outsourcing is selecting a service provider that understands your organization. A SOC 2 certification provides assurance on the Security, Availability, Confidentiality, Processing Integrity, and Privacy of information. If you are dealing with sensitive customer data, these elements are key success factors. In a SOC 2 report, the risk control framework is described, including the related controls and procedures for monitoring the risk control framework. The report is prepared in accordance with the Trust Services Criteria to provide a set of criteria for Security, Availability, Processing Integrity, and privacy to keep pace with the rapid growth of cloud computing and business outsourcing challenges provided by the global economy.

### Type I Report

A SOC 2 Type I report includes an opinion of an external auditor on the controls placed in operation at a specific moment in time. The external auditor examines whether the controls are suitably designed to provide reasonable assurance that the financial statement assertions are accomplished and whether the controls are in place.

### Type II Report

In a SOC 2 Type II report, the external auditor reports on the suitability of the design and existence of controls and on the operating effectiveness of these controls in a predefined period of six months minimum. This implies that the external auditor performs a detailed examination of the internal control of the service organization and also examines whether all controls are operating effectively in accordance with the predefined processes and controls.



# Key Benefits

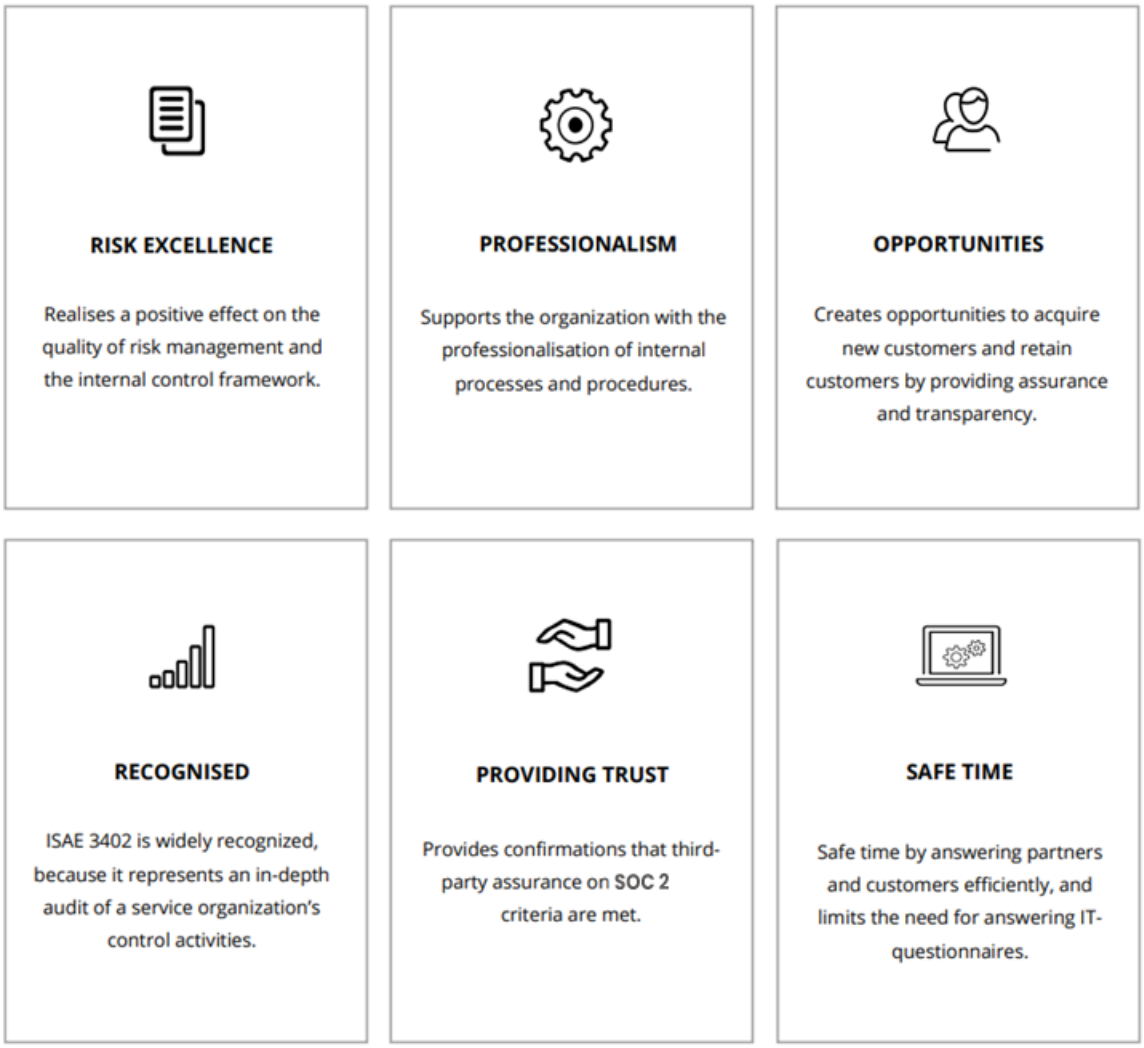
## Of SOC 2 Compliance

### Experience the Benefits of SOC 2 Reports

SOC 2 reports are used by organisations as a marketing tool. New and existing customers know immediately that they are dealing with a reliable party. Organisations that do not have such reporting may be missing out on important new opportunities.

### Advantage in Procurement

During the sales process, it is common for a customer to ask their supplier to fill in an IT questionnaire prepared by a team of engineers. Now, a SOC 2 report is likely to provide effective answers to these questions. It will speed up the process considerably. This will also give the customer the feeling and confidence that the processes are indeed in order.



# Introducing Securance

## Invest in Efficiency, Value, and Partnership

- **Analyse Risks**
- **Plan the Project**
- **Prepare System Descriptions**
- **Perform a Readiness Assessment**

**Implementing SOC 2 requires effective planning, leadership involvement, thorough analysis of processes and reliable resources and project management.**

Securance originates from a 'Big Four' audit firm and was founded in 2004. The result of our background is that we work in accordance with the highest professional standards and have experience in working with tight deadlines. We live by our professional standards and we always deliver the highest quality, whilst continuously striving to meet our clients' needs.

As a consequence of our flat structure and efficient communication framework, we can respond quickly to your requirements. Choosing Securance implies selecting a professional organisation, but also choosing for a personal approach. Effective project management, our experience with implementing risk management frameworks in your industry, and professionalism are in our opinion the foundation for excellent results.

As Securance, we believe that a good understanding, clear communication, and knowledge of our clients' industry are essential for delivering added value to you as our client. Based on this approach we will inform you on the relevant changes in laws, regulations and other important developments.

SECURANCE
BE SURE

# Our Satisfied Customers

## References












SECURANCE
BE SURE


## Securance Ltd.

**63-66 Hatton Garden**
**London EC1N 8LE, UK**
**+44 20 351 446 56**
**www.securance.co.uk**

## Securance - Seadot

**Sidenvävargatan 17**
**753 19 Uppsala**
**+46703040656**
**www.seadot.se**

## Securance BV

**Reactorweg 47**
**3542 AD Utrecht**
**+31 (0)30 2800888**
**www.securance.nl**