RISKLANE SOLUTIONS

info@risklane.com
www.risklane.com

STEP-BY-STEP GUIDE

SOC 2

COMPLIANCE

CONTENT

GETTING TO KNOW SOC 2

ALIGNING EXTERNAL REQUIREMENTS TO INTERNAL RISK EXCELLENCE

In this step-by-step guide, we will provide you with the necessary information on SOC 2. The guide consists of information regarding the SOC 2 standard and the Trust Services Criteria, the project phases of SOC 2 compliance (scope definition, implementation, and audit), and the benefits of SOC 2 for your organization.

As a professional Risk Management, Governance, and Compliance firm we are pleased to provide support with the SOC 2 compliance project within your organization. We are more than pleased to answer any questions you might have regarding SOC 2.

SOC 2 COMPLIANCE

OUTSOURCING | TRUST SERVICES CRITERIA

SOC 2 is a Service Organisation Control (SOC) report which provides assurance over outsourced processes. A audit performed in accordance with SOC 2 is widely recognized, because it represents an in-depth audit of a service organisation'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's non-financial reporting controls as they relate to Security, Availability, Processing Integrity, Confidentiality, and Privacy. These principles are outlined in the Trust Services Criteria. Each of the criteria has defined requirements (Points of Focus) which must be met and implemented within the organisation 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 services organisation. The only criteria that is mandatory for SOC 2 is the Security criteria. These criteria are also referred to as the common criteria. Additional criteria can be included within the scope of a SOC 2 reporting.

COMMON CRITERIA

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.

PROJECT PHASES

PHASE 1
PREPARING THE SCOPE OF THE SOC 2 REPORT

PHASE 2
IMPLEMENTING SOC 2 WITHIN YOUR ORGANISATION

PHASE 3
SOC 2 AUDIT PROCEDURES

TRUST SERVICES CRITERIA

CRITERIA EXPLAINED

The only mandatory criteria is the Security (Common) 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 organisation 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

Information and systems are protected from unauthorised access, unauthorised disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality and privacy of information or systems and impair the entity's ability to accomplish its purpose.

AVAILABILITY

Availability refers to controls that demonstrate that systems remain operational and perform to meet established business objectives and service level agreements. Information and systems are available for operation and use to achieve the entity's purpose.

CONFIDENTIALITY

Information that is considered confidential is protected to meet the objectives of the entity. Confidentiality requires companies to demonstrate their ability to safeguard confidential information throughout its lifecycle, including its collection, processing and disposal.

PROCESSING INTEGRITY

The use of the system is complete, accurate, valid, timely and authorised to meet the entity's purpose. Controls and thorough policies and procedures (e.g. backup/restore) are implemented to ensure the accuracy and completeness of information.

PRIVACY

Personal data is collected, stored, disclosed, used, and disposed of in order to fulfil the entity's purpose. Availability and business continuity controls are implemented to guarantee that products and services are available to authorized individuals when needed.

PHASE 1. SCOPE DEFINITION

APPLICABLE TRUST SERVICES CRITERIA

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 an scope section that note 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 the software application(s), 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 focus on the service organisation’s operations and services provided to customers. 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.

COMPETETIVE ADVANTAGE

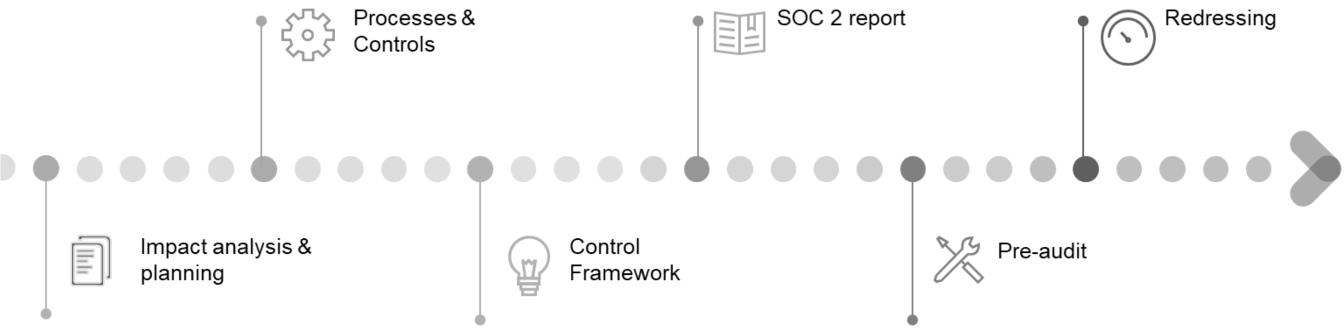
SOC 2 PROVIDES A COMPETITIVE ADVANTAGE BY DISTINGUISHING SERVICE ORGANISATIONS FROM THEIR COMPETITORS.

BENEFITS OF SOC 2 REPORTS RANGE FROM STRENGTHENING AND REFINEMENT OF RISK MANAGEMENT, TO GAINING CONFIDENCE IN MARKETS BY TRANSPARENCY OF THE CONTROL FRAMEWORK.

SOC 2 CREATES AUDIT EFFICIENCY AND REDUCTION OF BUSINESS INEFFICIENCIES.

PHASE 2. IMPLEMENTATION

STEP-BY-STEP-APPROACH



01 IMPACT ANALYSIS & SCOPING

In Phase 1, the impact (GAP analysis) of the implementation is 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.

02 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 organisation. The organisation 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. Proactive advise on the implementation of any missing controls (including process descriptions) will be provided during this phase.

ALIGNING THE CONTROL FRAMEWORK TO STRATEGIC OBJECTIVES

Personal approach
Professional results

03 CONTROL FRAMEWORK

In Phase 3, the internal control framework will be described based on the most recent COSO framework (COSO 2013) and the general section of the reporting is prepared. In the general section a description of the processes, the organisation and the General IT Controls is included.

04 SOC 2 REPORT

In Phase 4 the complete 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, which is discussed in detail with relevant staff. The organisation implements any identified problem areas and associated missing controls within the organisation during this phase.

05 PRE-AUDIT

After the preparation of the report, a pre-audit or 'walkthrough' is carried-out 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 organisation will provide the documentation and evidence required.

06 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. Solutions are provided that can be implemented within the organisation and the SOC 2 report. Phase 6 will result in the final SOC 2 report.

LEAD TIME

In general, 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 employees is expected to be one to two days per week during that period.

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 to successful outsourcing is selecting a service provider that understands your organisation. A SOC 2 report 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.

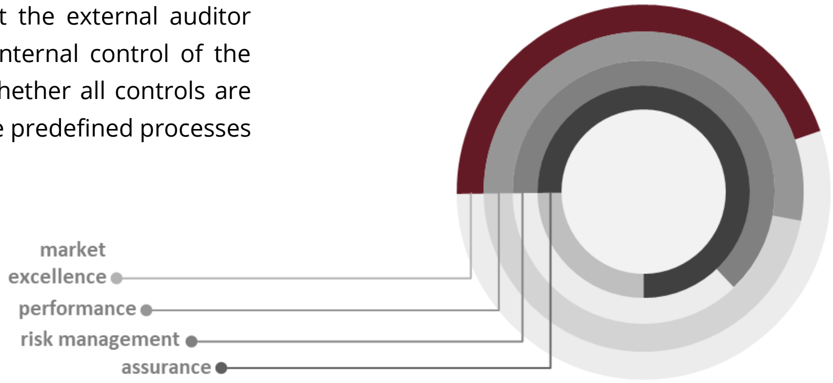
Minimizing business disruption by **effective** project management

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 three months minimum. This implies that the external auditor performs a detailed examination of the internal control of the service organisation 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

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

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 provide the customer the feeling and confidence that processes are indeed in order.

RISK EXCELLENCE

Realises a positive effect on the quality of risk management and the internal control framework.

PROFESSIONALISM

Supports the organization with the professionalisation of internal processes and procedures.

OPPORTUNITIES

Creates opportunities to acquire new customers and retain customers by providing assurance and transparency.

RECOGNISED

SOC 2 is widely recognized, because it represents an in-depth audit of a service organization's control activities.

PROVIDING TRUST

Provides confirmations that third-party assurance on security, availability, confidentiality, processing integrity, and privacy criteria are met.

SAFES TIME

Safes time by answering partners and customers efficiently, and limits the need for answering IT-questionnaires.

INTRODUCING RISKLANE

INVEST IN EFFICIENCY, VALUE, AND PARTNERSHIP

» ANALYSE RISKS
» PLAN THE PROJECT
» PREPARE SYSTEM DESCRIPTIONS
» PERFORM A READINESS ASSESMENT

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

Risklane originates from a ‘Big Four’ audit firm and is 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 Risklane implies selecting a professional organisation, but also choosing for a personal approach. In our opinion, effective project management, our experience with implementing risk management frameworks in your industry, and professionalism are the basis for excellent results.

As Risklane, we also feel 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.

OUR SATISFIED CUSTOMERS

REFERENCES

FUJITSU

colt

Planday

NTT

CSC

Templafy

CUSHMAN & WAKEFIELD

axians

Aareon

eurofiber

LIBERTY GLOBAL

Canon

RISKLANE

MANAGE RISK AND RESULT

Risklane Ltd.
1 Fetter Lane
London EC4A 1BR, UK
+44 20 351 446 56
www.risklane.com

Risklane BV
Reactorweg 47
3542 AD Utrecht
+31 (0)30 2800888
www.risklane.nl