SOC Audit Services

A framework for auditing service organisations, focusing on non-financial reporting controls.

GLOBAL COMPLIANCE CERTIFICATION
GCC

SOC is an essential tool in today's business landscape.

Contents

SOC Definition

« BACK TO CONTENTS

The System and Organisation Controls (SOC) framework is an essential tool in today's business landscape, providing a structured approach to evaluating and reporting on the effectiveness of an organisation's internal controls.

SOC Definition Continued

« BACK TO CONTENTS

Developed by the American Institute of CPAs (AICPA), the SOC framework offers a comprehensive set of standards and guidelines that help organisations address key areas of concern, including financial reporting, data security, privacy, and operational integrity.

There are several types of SOC reports, each tailored to different needs and objectives, SOC 1, SOC 2, SOC 2 Plus, SOC 3, SOC for Cybersecurity, and SOC for Supply Chain.

The main SOC reports are as follows:

SOC 1

This report focuses on controls relevant to financial reporting. It is often used by service organisations that provide services impacting their client's financial statements, such as payroll processing or data centre operations. SOC 1 reports help assess the reliability of these services and the controls in place to ensure accurate financial reporting.

SOC 2

SOC 2 reports are more comprehensive and cover a broader range of criteria, known as Trust Service Criteria (TSC). These criteria include security, availability, processing integrity, confidentiality, and privacy. SOC 2 reports are commonly used by service providers, cloud computing vendors, and other organisations to demonstrate their commitment to data security and privacy.

SOC 3

SOC 3 reports are designed for public use and provide a high-level summary of an organisation's controls related to security, availability, processing integrity, confidentiality, and privacy. They are often used for marketing purposes or when organisations want to assure customers and stakeholders of their adherence to SOC standards without disclosing detailed control information.

The AICPA's SOC framework provided a structured approach to evaluating the effectiveness of a service organisation's controls, offering greater assurance to client businesses.

Harry Khalili
Chartered Accountant
AICPA – International Associate

Mousa Sharifi
Managing Director
AICPA – Affiliate member

What is Involved in a SOC Audit

« BACK TO CONTENTS

Service organisations

Service organisations are entities that provide services to other businesses, such as cloud storage providers, data centres, or payroll processing companies. These services often involve access to sensitive client data, making robust control systems crucial for ensuring its security and integrity.

American Institute of Certified Public Accountants (AICPA)

The American Institute of Certified Public Accountants (AICPA) is a professional organisation founded in 1887 in the United States. It is the world's largest member association representing the accounting profession, with more than 428,000 members. The AICPA administers the Uniform CPA Examination and provides comprehensive guidance documents and frameworks.

Through its initiatives, the AICPA establishes a consistent and dependable foundation for accounting practices. It offers specialty credentials for CPAs specialising in areas such as personal financial planning, forensic accounting, business valuation, information management, and technology assurance.

SOC 2 Examination

A SOC 2 examination, also known as a SOC 2 audit, is an independent and rigorous review conducted by a qualified professional. This examination assesses the effectiveness of a service organisation's controls relevant to the **Trust Service Principles (TSPs)** outlined by the AICPA.

The examination can only be conducted by qualified professionals with the necessary expertise.

- **US-Based Engagements:** Independent Certified Public Accountants (CPAs) or CPA firms licensed within the United States and adhering to AICPA standards are responsible for conducting SOC 2 examinations. SOC 2 examinations should adhere to the **Statement on Standards for Attestation Engagements (SSAE) 18**, specifically sections AT-C 105 and 205.
- **International Engagements:** The examination may also be performed by a qualified professional accountant (CPA/CA) acting in public practice, licensed in a jurisdiction outside the US. In this case, the examination must be conducted in accordance with ISAE 3000 or equivalent local country standards.

What is Involved in a SOC Audit Continued

« BACK TO CONTENTS

Role of the Service Auditor (CPA)

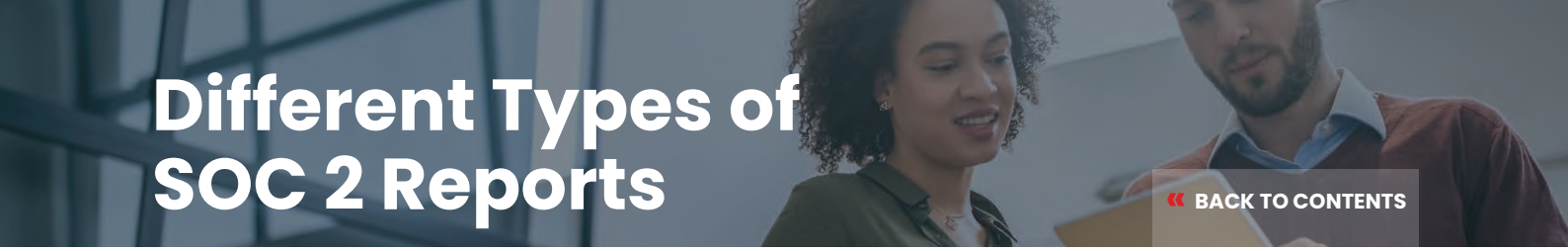
During the examination, the qualified professional (acting as the service auditor) expresses an opinion on the effectiveness of the service organisation's control environment. This opinion is based on an assessment of several key areas:

- **Description Criteria Compliance:** The auditor evaluates whether the service organisation's description of their systems and controls meets the established criteria for the chosen Trust Service Principles.
- **Control Design Effectiveness:** The auditor assesses whether the controls designed by the service organisation are appropriate and provide reasonable assurance for achieving service commitments and system requirements.
- **Control Operational Effectiveness (Type 2 Only):** For SOC 2 Type 2 examinations, the auditor goes beyond design and evaluates whether the controls are functioning as intended and consistently achieving the service organisation's objectives aligned with the chosen Trust Service Principles.

Categories of AICPA Trust Service Criteria (TSC)

The TSC framework comprises five main categories. Each category of TSC aligns with one or more of the SOC2 principles, each representing a core aspect of trustworthiness in service organisations:

1. **Security:** Focuses on protecting systems and data against unauthorised access, breaches, and cyber threats. Includes controls such as access control, encryption, network security, and incident response.
2. **Availability:** Ensures that systems and services are available and operational when needed by users. Covers aspects like redundancy, failover mechanisms, disaster recovery planning, and uptime monitoring.
3. **Processing Integrity:** Emphasises the accuracy, completeness, and validity of data processing. Includes controls for data validation, error detection and correction, system integrity checks, and transaction processing.
4. **Confidentiality:** Addresses the protection of sensitive information from unauthorised disclosure. Involves controls such as data encryption, access restrictions, data masking, and confidentiality agreements.
5. **Privacy:** Focuses on the management and protection of personal information in compliance with applicable privacy laws and regulations. Covers areas like consent management, data minimisation, data subject rights, and privacy policies.



Different Types of SOC 2 Reports

« BACK TO CONTENTS

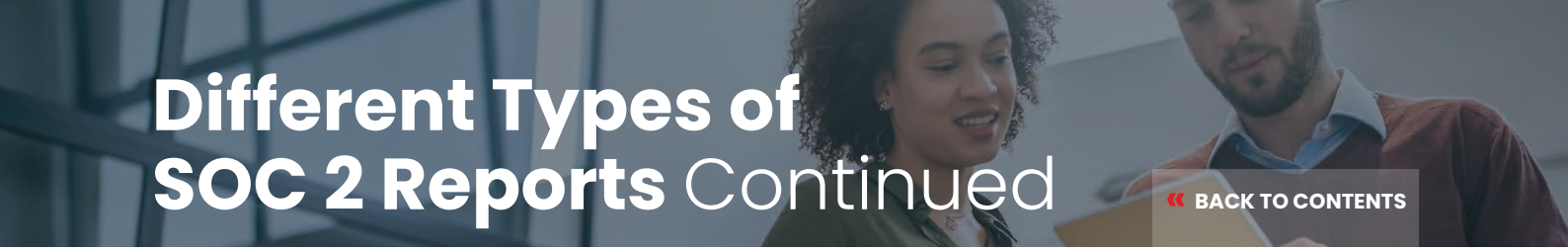
Type 1 Report

A Type 1 SOC 2 report evaluates the design and implementation of controls at a specific point in time. It provides a snapshot of the organisation's control environment and assesses whether controls are suitably designed to meet the specified criteria.

Type 2 Report

A Type 2 SOC 2 report provides a more comprehensive assessment by evaluating the effectiveness of controls over a specified period (typically six months or more). It not only assesses control design but also tests the operational effectiveness of these controls, providing a more in-depth understanding of the organisation's control environment and its ability to maintain compliance over time.

	Type 1 Report	Type 2 Report
1	Management's description of the system as of **a point in time** in accordance with the description criteria.	Management's description of the system **throughout a period of time** in accordance with the description criteria.
2	Management assertion that addresses: a) Whether the description of the service organisation's system as of **a point in time** is presented in accordance with the description criteria and; b) Whether the controls stated in the description were suitably designed as of **a point in time** to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria.	Management assertion that addresses: a) Whether the description of the service organisation's system **throughout a period of time** is presented in accordance with the description criteria; b) Whether the controls stated in the description were suitably designed **throughout a period of time** to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria, and; c) **Whether the controls stated in the description operated effectively throughout a period of time to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria.**
3	The service auditor's opinion about whether: a) The description of the service organisation's system as of **a point in time** is presented in accordance with the description criteria and; b) The controls stated in the description were suitably designed as of **a point in time** to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria.	The service auditor's opinion about whether: a) The description of the service organisation's system **throughout a period of time** is presented in accordance with the description criteria; b) The controls stated in the description were suitably designed **throughout a period of time** to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria, and; c) **The controls stated in the description operated effectively throughout a period of time to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria.**
4	Description of the service auditor's tests of controls and results thereof: - Design and implementation - **As of a specific date** - **May take 2-3 months** - This report **does not include** tests of controls or the results of such tests.	Description of the service auditor's tests of controls and results thereof: - Design, implementation, **and operating effectiveness** - **For a stated period** - **May take 6-12 months** - This report **includes** tests of controls or the results of such tests.
5	Suitable for: • Organisations seeking a preliminary evaluation of their control environment. • Companies preparing for a more comprehensive Type 2 examination in the future. • Stakeholders who need assurance about the design of controls but not their operational effectiveness. • A new service organisation looking to quickly demonstrate control design.	Suitable for: • Organisations requiring a thorough evaluation of their control environment. • Companies needing to demonstrate ongoing compliance and effectiveness of controls to clients and regulators. • Stakeholders seeking assurance about the reliability and robustness of the organisation's control practices over time. • Provides ongoing assurance over a period, suitable for established organisations.



Different Types of SOC 2 Reports Continued

« BACK TO CONTENTS

Report Sections

The following table outlines the SOC2 report sections and the responsible entity:

Section	Description	Responsibility
1: Independent Service Auditor's Report	- Provides the scope and opinion of the service auditor regarding the assertion and system description. - Evaluates design and operating effectiveness (Type 2 only) to meet control objectives.	Service Auditor (CPA)
2: Management's Assertion	- Presents facts and assertions made by management regarding the audited system(s).	Service Organisation
3: Description of the System	- Details the system(s) being reported, including boundaries, infrastructure, controls, commitments, and other relevant information. - Information included in this section must be auditable to ensure service commitments and system requirements align with criteria.	Service Organisation
4: Auditor's Tests of Controls and Results (Type 2 Only)	Typically displays four columns: - Objectives related to the report's criteria. - Controls implemented by the service organisation. - Auditor's tests of these controls. - Results of the tests.	Service Auditor (CPA)

Needs and Benefits

BACK TO CONTENTS

The Need for SOC 2 Reports in Today's Business Landscape

In today's digital business landscape, cybersecurity threats are a significant concern for organisations of all sizes. Data breaches, cyberattacks, and regulatory requirements demand a higher level of accountability and transparency regarding data protection measures. SOC 2 reports are essential because they demonstrate that a service organisation has implemented and maintained effective controls to safeguard client data, ensure service availability, maintain processing integrity, protect confidentiality, and adhere to privacy requirements. These reports are crucial for building trust with clients, winning new business opportunities, and meeting regulatory compliance obligations.

The AICPA Trust Service Principles (TSP) form the foundation of SOC 2 audits. These principles are Security, Availability, Processing Integrity, Confidentiality and Privacy.

Benefits of SOC 2 Examination for Service Organisations

- **Enhanced Trust:** SOC 2 Examination enhances trust and confidence among clients and stakeholders by demonstrating a commitment to security, privacy, and operational excellence. It assures clients that their data and services are in capable hands.
- **Competitive Advantage:** Having SOC 2 reports can give service organisations a competitive edge. Many clients now require SOC 2 compliance as a prerequisite for doing business, so a SOC 2 Report can open doors to new opportunities and markets.

gccertification.com

GLOBAL COMPLIANCE CERTIFICATION
GCC

JAS-ANZ
WWW.JAS-ANZ.ORG/REGISTER

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
IAF

HEAD OFFICE
Level 1, 77 Pacific Highway
North Sydney NSW 2060
Australia
T 1800 444 800

UNITED STATES
300 Spectrum Center
Drive, Suite 400, Irvine,
CA 92618
T +1 800 400 9594