System and Organisation Controls 2: A Guide to SOC 2 Audits

DATE: April 2025
VERSION: 1.0

TABLE OF CONTENTS

Introduction

The System and Organisation Controls (SOC) 2 framework was developed by the American Institute of CPAs (AICPA), the national organisation for Certified Public Accountants (CPAs). However, the framework is not only relevant to the USA and organisations based there.

A big driver for SOC 2 compliance in Europe is US firms looking for assurance from their European supply chain partners, making SOC 2 compliance increasingly relevant in sectors such as Defence, Health, Finance, and Technology.

A SOC 2 audit comprehensively evaluates an organisation's internal security controls regarding managing and protecting sensitive data. It is carried out by independent auditors, providing transparency and assurance to clients, customers, and partners that an organisation has robust and secure processes to secure and hold sensitive data. The audit process assesses the design and operational effectiveness of the organisation's controls over time, helping to build trust and mitigate risks associated with data breaches, service interruptions, or non-compliance with industry regulations.

Additionally, the paper will demonstrate how the SOC 2 framework aligns with established cybersecurity frameworks and regulations such as ISO 27001 and GDPR.

The SOC 2 Framework

The SOC 2 framework focuses on five key principles. The Trust Services Criteria (TSC) which are made up of the following:

- **Security**.
  - The protection of systems and data from unauthorised access, breaches, or other cyber threats. It includes measures like firewalls, encryption, access controls, and vulnerability management
- **Availability**,
  - Ensuring that systems are available for operation as expected, without unexpected or long-lasting outages. This allows an organisation to meet its service commitments and performance objectives.
- **Processing integrity**,
  - This involves ensuring system processing is complete, accurate, timely, and authorised. It ensures that data is processed as expected, without errors or interruptions, and according to the organisation's and its clients' specifications.
- **Confidentiality**,
  - Protecting sensitive data from unauthorised access or disclosure. Data must be secured so that only those who need to know can access it with proper authorisation and access control.
- **Privacy**.
  - The collection, use, retention and destruction of personal information. Ensuring compliance with privacy laws and regulations such as GDPR to protect personal information from misuse.

Our Methodology

There are two types of SOC 2 attestation reports: Type 1 and Type 2.

- **Type 1** audits and reports evaluate an organisation's security controls at a single point in time. These audits and reports take 4-6 weeks to complete and provide a snapshot of compliance against the TSC.

- **Type 2** audits and reports evaluate an organisation's compliance with the TSCs over a period of time, typically a year or a financial quarter. This means the audits and reports can take longer to complete than Type 1, but provides greater assurance of an organisation's compliance with SOC 2.

When carrying out SOC 2 audits, we employ a four-phase methodology.

1. **Gaining an Understanding of Internal Control**
    a. Kick-off meeting.
    b. Interviews.
    c. Policy review, guidance and recommendations.
    d. Perform an in-depth review of management's description of controls and observe operations.
2. **Testing**
    a. Inquiry.
    b. Observation.
    c. Inspection.
    d. Re-performance.
    e. Weekly status meetings throughout the testing process.

3. **Wrap-up/Review**
    a. Assist in drafting the report.
    b. Review and provide recommendations on the organisation's description of the system.
    c. The organisation reviews the draft.

4. **Reporting**
    a. Quality control.
    b. Review.
    c. Finalise the report.
    d. Management is asked to provide a management representation letter.

Mapping SOC 2 to Existing Frameworks

SOC 2 is a framework designed to assess how organisations handle data regarding the TSC set out in the framework. Other frameworks and regulations, such as ISO 27001 and GDPR, also examine data protection and controls with varying scopes and focus.

ISO 27001 is an organisational-wide framework that examines how organisations implement an Information Security Management System (ISMS) that provides a comprehensive governance framework and controls for information security across the organisation. To achieve ISO 27001 certification, an organisation must undergo annual audits from an independently qualified auditor to ensure that its ISMS conforms to the framework and is effective for the organisation.

GDPR is an EU and UK regulation governing the privacy and protection of personal data. It applies to all organisations handling the personal data of EU and UK residents, regardless of where the organisation is located. GDPR impacts businesses and organisations that may store, transmit, or

process personal data. Unlike SOC 2 and ISO 27001, organisations cannot choose not to comply with GDPR without repercussions, such as significant fines.

AMR CyberSecurity employs ISO 27001 Lead Auditors and experts on data security. We assist our customers in understanding the potential impacts of data security laws, regulations, and frameworks on their organisations while also providing assurance and advising them on becoming compliant.

Conclusion

The System and Organisation Controls (SOC) 2 framework is an internationally recognised assurance framework for demonstrating data security controls for an organisation.

With cyber threats evolving at an unprecedented pace, organisations must proactively adopt measures that protect their customers, operations, data, and reputation.

By partnering with us - a reputable cyber security consultancy organisation can navigate the complexities of SOC 2 compliance, enhance their cyber security posture, and contribute to a more secure data privacy world.

Together, we can build a more resilient and secure future.

How we can help

Navigating the complexities of System and Organisation Controls (SOC) 2 compliance can be daunting. At AMR CyberSecurity, we specialise in providing tailored cyber security consultancy services to ensure your organisation meets and exceeds the data security requirements of SOC 2.

Our expert team brings extensive experience in cyber security risk assurance and advisory services. We offer a comprehensive suite of services designed to enhance your compliance posture, mitigate risks, and safeguard your operations.

Supporting Services

- SOC 2 Type 1 and Type 2 Audit and Report
  - Complete a full audit and report on SOC 2 compliance as a Type 1 or Type 2 report.

- ISO 27001 Implementation and Gap Assessment
  - Implement and embed an ISO 27001-compliant Information Security Management System (ISMS).
  - Conduct an internal audit assessment of an organisation's ISMS to ensure compliance with the ISO 27001:2022 standard.
- GDPR Readiness
  - Assess and advise clients on their compliance and readiness to meet GDPR.
- NIST 800-57 Assessment
  - Conduct an assessment of an organisation's security controls against the NIST 800-57 standard.

Why AMR CyberSecurity?

We have partnered with a trusted AICPA-registered auditor and can therefore seamlessly manage the end-to-end process and provide attested SOC 2 reports.

AMR CyberSecurity will help you achieve robust security and compliance with SOC 2 reporting, allowing you to focus on your core business operations confidently.