NZ INFOSEC
SECURITY COMPLIANCE

SOC 2 Compliance

SOC - INTRODUCTION

SOC (Service and Organisation Control) for Service Organizations are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service. SOC reports are designed to help service organizations build trust and confidence in their service delivery processes and controls through a report by an independent AICPA Certified Public Accountant.

The AICPA has outlined 3 types of SOC reports that Each type of SOC report is designed to help service organizations meet specific user needs:

- SOC 1 Report – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
- SOC 2 Report – Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
- SOC 3 Report – Trust Services Report for Service Organizations

SOC 1, SOC 2, SOC 3 and Service Organization Control Reporting are registered service marks of the American Institute of Certified Public Accountants (AICPA).

SOC REPORTING

SOC1	SOC2	SOC3
Remains Focussed on internal controls related to financial reporting. SOC 1 is designed to review a financial and accounting controls. Restricted use.	A SOC 2 report is an examination on a service organization's controls over one or more of the following five (5) Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality and Privacy Detailed description of systems including controls to address the criteria. Restricted use.	Similar to a SOC 2, but for broader distribution. SOC 3 is likely to have some of the components of a SOC 2, it’s not going to be as comprehensive. Summary report. Unrestricted use and ability to display seal on a website.

SOC 2 TRUST SERVICE CRITERIA

SOC 2 is specifically designed for service providers storing customer data in the cloud. That means SOC 2 applies to nearly every SaaS company, as well as any company that uses the cloud to store its customers' information.

Domain	Principle
Security	The system is protected against unauthorized access (both physical and logical)
Availability	The system is available for operation and use as committed or agreed
Confidentiality	Confidential data is protected as committed or agreed
Process Integrity	System processing is complete, accurate, timely and authorized
Privacy	Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by AICPA and CICA

SOC 2 CATEGORIES TO BE INCLUDED

Category	Why to include?
Security	This category is required for all SOC 2 reports and is designed to prevent and detect system failure, incorrect processing, theft, or other unauthorized data removal.
Availability	Monitoring network performance and availability, site failover and security incidents response etc. This category is useful to include if customers ask you about downtime service-level agreements, uptime guarantees, a status page, and other accessibility requests.
Confidentiality	If your clients want data deleted when contracts end, have private or sensitive information stored in your company's platform, or require non-disclosure agreements when they do business with you or others, the Confidentiality category is vital to include in your SOC 2 report.
Processing Integrity	This shows system processing and data are complete, valid, accurate, timely, and authorized to meet objectives. If your company is a data pipeline platform or offers a payment system of some kind, your customers likely rely on you for data processing. That means the Processing Integrity category may be one of the TSC within your SOC 2 report.
Privacy	When clients store personally identifiable information or sensitive personal data (e.g., social security numbers, financial information, etc.), you may want to include this TSC in your SOC 2 report.

SOC 2 CERTIFICATION / REPORT

- SOC 2 certification / report is issued by a third-party auditor (AICPA CPA).
- There are two types of SOC reports:
    - SOC 2 Type I report is an attestation of controls at a service organization at a specific point in time. It describes a clients' systems and whether their design is suitable to meet relevant trust principles.
    - SOC 2 Type II report is an attestation of controls at a service organization over a minimum six-month period. It details the operational effectiveness of those systems.
- We provide gap assessment, remediation and readiness support for SOC 2.
- SOC audits are done by an AICPA certified CPA.
- CPA details can be verified from www.cpaverify.org as recommended on AICPA website - www.aicpa.org/forthepublic/findacpa.html.

SOC 2 CERTIFICATION TIMELINE

STEP 1

1. Development of policies, procedures, processes, staff training - 2 to 3 months *(Client dependent)*

STEP 2

SOC 2 Type 1 Audit (2-4 days) , SOC 2 Type 1 Report (1-2 weeks)

STEP3

Maintain the SOC 2 policies, procedures, logs for minimum 6 months *(Client dependent)*

STEP 4

Preparation for Type 2 Audit - Evidences, logs, documents etc. *(Client dependent)*

STEP 5

SOC 2 Type 2 Audit (2-4 days) , SOC 2 Type 2 Report (1-3 weeks)

SOC 2 reports are required annually so it is important to maintain it.
SOC 2 is not a legal or a mandatory requirement.

Thank You

Information Security Is Everyone’s Responsibility

www.nzinfosec.co.nz