HEALTH-CHECK
SOC 2 TRUST SERVICES CRITERIA

assurancelab

Trusted assurance solutions

CompanyX
November 3, 2020

John,

Thank you for completing our SOC 2 Health-check assessment. The enclosed report provides an overview of your level of controls maturity with respect to the SOC 2 Trust Services Criteria and an assessment of the common areas of control gaps. We have provided a summary of this assessment, guidance on the Trust Services Criteria areas and an overview of SOC 2 and our services that may follow this assessment. To proceed to a SOC 2 attestation report, we recommend completing our full assessment process that will provide a listing of all identified controls and observations with respect to the SOC 2 criteria.

To get started with a full SOC 2 assessment or other services to support your SOC 2 requirements, contact us today.

Paul Wenham

Founder & CEO
E: paul@assurancelab.com.au
P: +61(0)490 086 000
W: https://assurancelab.com.au

Disclaimer: This report does not constitute an assurance engagement, nor an opinion by AssuranceLab on the controls, descriptions or other contents of this report. CompanyX remains wholly responsible for the completeness, accuracy and appropriateness of this report and any related security and compliance objectives.

SOC 2 HEALTH-CHECK REPORT

Overview

The Assessment Summary below includes a rating of your control maturity, recommendations for any improvements identified and a score for each area. Benchmarking is provided in the following section to compare the control maturity to peers.

Scoring guide:

- A score of 100% indicates you are well placed to complete a SOC 2 attestation.
- Between 50-100% may require further actions to achieve the SOC 2 criteria.
- Less than 50% will not achieve the SOC 2 criteria until further actions are taken.

Trust Services Criteria

All SOC 2 reports include the Trust Services Criteria for Security/Common Criteria. These criteria form the basis of compliance with the SOC 2 standard. They used to support the additional criteria for Availability, Confidentiality, Privacy and Processing Integrity. These additional areas are optional for the Service Organisation to include or exclude. The decision should be informed by the nature of the services and the expectations or preferences of end users of the SOC 2 report(s). Based on your inputs to the Trust Services Criteria assessment section, we recommend you consider the inclusion of the following additional criteria areas:

> **Availability:** Recommended inclusion based on the critical nature of your systems and services. Where an outage would have a significant impact on the users, Availability is typically expected to be included by users of the SOC 2 report.
>
> **Privacy:** In order to demonstrate your GDPR compliance, you may include a disclosure in the unaudited section (Section V) of SOC 2 report(s). As your end users do not have high-risk personal data and strict privacy obligations, this disclosure is the recommended approach rather than inclusion of the Privacy area in the formal attestation. There is no cost for including this privacy disclosure.

The choice of criteria should be discussed with the Service Auditor prior to finalising any commitment to end users. Generally the scope of criteria is flexible to change up to the point of issuing your SOC 2 report(s). A common strategy is to start with a lesser scope with plans to expand in subsequent SOC 2 reports, if required.

Assessment Summary

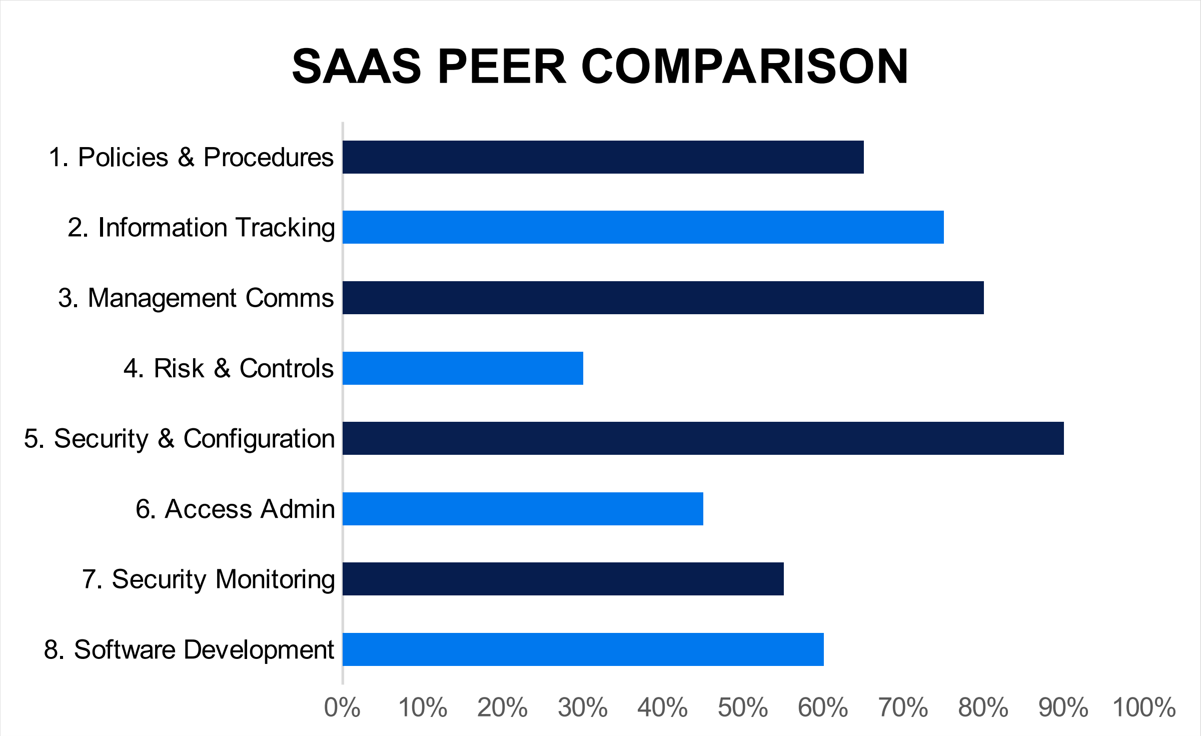
Section	Summary	Score
1. Policies and Procedures	**Control maturity:** Above average You have defined and documented most of the policies and procedures assessed for SOC 2. **Recommendation(s):** Consider documenting the following policies or procedures: • Customer contracts/agreements,Customer/user support,Risk management,Business continuity & disaster recovery.	65%
2. Information Tracking	**Control maturity:** Above average You maintain information tracking to support internal controls for most areas reviewed in a SOC 2 assessment. **Recommendation(s):** Consider implementing software, tools or logs to track and monitoring the following: • System events/failures,Control failures/policy breaches.	70%
3. Management Communications	**Control maturity:** Above average You are applying most of the common good practice approaches to management and communications. **Recommendation(s):** Consider implementing the following practices: • Senior Management meetings,Intranet/shared drive for document sharing,Documented org chart and job descriptions.	60%
4. Risk & Control Assessments	**Control maturity:** High You have a well-structured approach to risk management to support SOC 2 compliance.	100%

Section	Summary	Score
5. System Security & Configurations	**Control maturity:** Above average You apply some of the security and configuration settings to protect the systems and data from unauthorised access. **Recommendation(s):** Consider implementing the following security improvements: • Strong authentication controls (MFA or strong password requirements),Anti-virus software on company devices,Mobile device management and security restrictions.	60%
6. Access Administration	**Control maturity:** Above average You apply some of the required access administration procedures. **Recommendation(s):** Consider implementing formal documented procedures for the following areas: • Restrict administrator access to authorised personnel,Define access roles that require segregation.	80%
7. Security & System Monitoring	**Control maturity:** Above average You apply some monitoring practices to review the system performance and security. **Recommendation(s):** Consider implementing the following monitoring practices: • Review of compliance with policies (at least annually),System monitoring: performance, capacity, uptime.	80%

Section	Summary	Score
8. Software Development	**Control maturity:** Above average You have most of the requisite change management processes to support SOC 2 compliance. **Recommendation(s):** Consider implementing the following practices for all software and infrastructure configuration changes: • Acceptance criteria,Communications to impacted users.	80%

BENCHMARKING

The following graph provides the average scores for the software as a service (SaaS) industry based on past completed assessments. These can be compared to the scores in the table above for consideration of how your control maturity compares. For any specific insights on industry practices, contact us to discuss further.



NEXT STEPS

We tailor our approach to each organisations' requirements. We generally recommend the following steps:

1. **Consultation:** Contact us for a free consultation, quote and guidance on the best path to meet your SOC 2 needs;
2. **Readiness Assessment:** Complete our full SOC 2 assessment to identify any control gap observations and generate a complete listing of your control processes and evidence requirements for the SOC 2 audit;
3. **Type 1 Audit:** Conduct a SOC 2 Type 1 Audit engagement to demonstrate compliance by design (optional);
4. **Type 2 Audit:** Conduct a SOC 2 Type 2 Audit engagement covering your desired period of time (3-12 months) to demonstrate continuous compliance over the period

assurancelab

HQ: Level 3/11 York Street, Sydney
E: info@assurancelab.com.au
M: +61(0) 490 086 000

AssuranceLab
ABN: 35623143831