SOC 2 Compliance

What SOC Compliance Means to You

Are Cloud/SaaS vendors “Walking the Walk” with your data?

Introduction

Many businesses are poised for growth; their market is solid, their products/services are in demand and their reputation is favorable, yet they run into a roadblock. That roadblock is the capital expense of upgrading their business systems (especially CRM) and the required IT infrastructure to support the planned growth. As businesses look for routes around this roadblock, moving to the Cloud or a Software as a Service (SaaS) model can be a viable option.

A key benefit of the Cloud or SaaS is that it enables you to subscribe to the service much like a mobile phone plan, paying for just what you need without a large up-front capital expense. If you need additional services or to add additional employees, you can simply add them to your plan. CRM solutions are ideal candidates for this service.

SOC Compliance

IF YOU HAVE MADE THE DECISION TO MOVE TO THE CLOUD AND ARE BEGINNING THE CLOUD/SAAS VENDOR SELECTION PROCESS, YOUR NEXT CONSIDERATION IS TO IDENTIFY A VENDOR WHO YOU CAN TRUST WITH YOUR PROPRIETARY BUSINESS DATA AS WELL AS YOUR REPUTATION. BELOW ARE SOME KEY CONCERNS THAT MUST BE TOP OF MIND WHEN CONSIDERING VENDORS.

Security and accessibility of your business data

Consistent and secure data backups with a recovery process

Protection of confidential information (yours and your clients')

Protection of your customers' privacy

The challenge becomes how to verify that a Cloud/SaaS provider addresses and resolves these concerns to an acceptable standard. Do you know the acceptable standard? Most do not.

You can meet this challenge head-on by asking vendors if their solutions and processes are SOC Compliant.

Let us pause a moment and discuss exactly what SOC is and why it should be important in your Cloud/SaaS vendor selection.

SOC is the acronym for Service Organization Control (A vendor providing you SaaS is a Service Organization).

Name of Report	Description
SOC 1	✓ Report focuses on financial reporting and related processes/controls ✓ Very detailed ✓ Normally restricted and access requires a non-disclosure agreement (NDA) ✓ Not relevant to a Cloud/SaaS service provider
SOC 2	✓ Report focuses on processes and controls to insure all five Trust Service principles are met (Security, Privacy, Availability, Processing Integrity, Confidentiality) ✓ Very detailed ✓ Normally restricted and access requires a non-disclosure agreement (NDA) ✓ Created specifically for Cloud/SaaS providers
SOC 3	✓ Report also focuses on Cloud/SaaS providers and the five trust principles above. ✓ Does not provide detailed description of processes and controls ✓ Normally not restricted and can be shared ✓ Created specifically for Cloud/SaaS providers

Note: The SOC 2 and SOC 3 audit processes are identical; the difference is the level of detail in the report. In many cases, a Cloud service provider will ask for both reports based on the same audit.

Attaining SOC 2 Compliance is a rigorous audit process conducted by an independent agency certified by American Institute of CPAs. The audit process and focuses on five “trust principles” (see below) and each principle may have up to 90 sub-categories. Each sub-category targets a specific area of the SaaS provider’s Cloud process and has proof points. An artifact(s) is required to validate each proof point.

The audit spans the entire spectrum of the SaaS provider’s service offering, including technical data security, disaster recovery, business continuity, physical security, human resourcing, related business process, and much more.

The Trust Principles

MANY ORGANIZATIONS HAVE OPTED TO HAVE THEIR CRM SOLUTION HOSTED FOR A SERVICE FEE. THIS OPTION IS PREFERRED OVER INSTALLING THE CRM SOLUTION ONSITE FOR MANY REASONS.

Trust Principle	High-Level Standard
Security	✓ The system is protected against logical and physical unauthorized access.
Availability	✓ The system is available for operation and use as committed or agreed to.
Processing Integrity	✓ The system processes are complete, timely, accurate, and authorized.
Privacy	✓ The information considered “confidential” is protected as committed or agreed to.
Confidentiality	✓ Personal information that is collected, used, retained, or disclosed conforms to the commitments in the company’s privacy notice and conforms to the privacy principles of the American Institute of Certified Public Accountants (AICPA).

Audit Process

To become SOC 2 compliant, the SaaS provider must not only "talk the talk", but must "walk the walk" meaning a provider may have great processes and controls on paper, however, the must work in real life with a customer data? Hence, attaining initial SOC 2 compliance is a two-audit process.

Type 1 Audit

The very first audit referred to as a Type 1 Audit evaluates the provider's controls (processes) to validate that their design adheres to the mandated principles and standards at the time of the audit – "Talk the talk."

Type 2 Audit

The second audit referred to as a Type 2 Audit is conducted at least four months after the Type 1. It confirms that the controls (processes) evaluated in the Type 1 Audit function as designed on a day-to-day basis – "Walk the walk".

Once the Type 2 Audit is complete and the final report is completed, the provider is considered compliant assuming that there were no issues or deficiencies noted. To remain compliant, an annual audit is required to confirm all controls (processes) are in place and functioning.

It's important to note that the report dates can be confusing while reviewing either audit report provided by a vendor. For example, an audit completed in December 2019 reflects the the audit period of December 2018 to November 2019. This means that while the report is available in 2020, it may look as if it is outdated. Remember the audit validates all controls are still compliant and have been working as designed.

Conclusion

As you can see, selecting a SOC 2 Compliant Cloud/SaaS vendor is crucial to ensure the lifeblood of your business, your data and your reputation, are safe.

Act! is a flexible CRM solution designed for SMBs and is available in the Cloud. Act! SaaS controls (processes) have been SOC 2 compliant since 2017. Both single-tenant and multi-tenant Cloud options will provide a compliant platform, leaving you free to focus on your company's success.

A personal note about the audit process from the author:

While obtaining SOC 2 Compliance, Act! provides over 500 artifacts to support our controls for each audit. All audits are conducted onsite, taking about three days, and the auditors then require approximately six weeks to review all artifacts and complete the report. While the process is certified by AICPAs, the auditors include IT/Software security professional with substantial credentials.

What is Act!?

Purpose-built for small businesses, Act! combines proven CRM with powerful Marketing Automation, providing you with the ultimate toolset to drive business growth.

Growth made easy
CRM & Marketing Automation built for small & midsized business success.

To learn more about Act! visit
www.act.com

Or call us at

866-873-2006

Connect with Act!

8800 N. Gainey Center Dr., Suite 200 | Scottsdale, AZ 85258 | act.com