



SOC 2 Compliance

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





Introduction

Many businesses are poised for growth; their market is good, 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 its IT infrastructure to support the planned growth. These businesses must look for routes around this roadblock. In today's world, moving to the Cloud or a Software as a Service (SaaS) model is a viable option around the roadblock.

A key benefit of the Cloud is you can subscribe to the service much like a mobile phone plan, paying for what you need and not a large up-front capital expense. If you need additional services or to add additional employees, simply add to your plan. CRM solutions are ideal candidates for this service.

SOC 2 Compliance

Assuming you have made the decision to move to the Cloud and are beginning the Cloud/SaaS vendor selection process. I think we can agree that you need to completely trust the selected vendor with your business data and your reputation, therefore, here 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 your and your customers' confidential information.
- Protection of your customers' privacy.



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

However, you can meet this challenge head on by asking the vendor if their solution and processes are SOC 2 Compliant.

Let us pause a moment and discuss exactly what SOC 2 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).
- The 2 refers to Trust Services Criteria (this is desired for SaaS).
- Coupled they are referred to as SOC 2.

Attaining SOC 2 Compliance is a rigorous audit process conducted by an independent agency certified by American Institute of CPAs. It is a two-audit process and focuses on five "trust principles" (see below) and each principle may have up to 35 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, 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).

Two-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, do they work in real life with a customer’s data? Hence, SOC 2 is a two-audit process.

The first audit referred to as a Type 1 Audit evaluates the providers controls (processes) to validate they adhere to the mandated principles and standards at the time of the audit – “Talk the talk”.

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 completed the provider is considered compliant assuming that there were no issues or deficiencies noted. To remain compliant, an annual audit is required.

Conclusion

As you can see, selecting a SOC 2 Compliant Cloud/SaaS vendor is mandatory to attain peace of mind that the lifeblood of your business, data, and reputation are safe.

For general information, there is a SOC 1 Audit focused on internal financial processes and financial accountability. SaaS providers are not usually candidates for this audit. There is also a SOC 3 Audit report that provides larger organizations an external facing audit report.

Act! is a flexible CRM solution designed for SMBs and is available in the Cloud. Swiftpage’s SaaS controls/processes successfully underwent the SOC 2 Audit process from June 2017 to November 2017. Both single-tenant and multi-tenant Act! 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, Swiftpage provided over 450 artifacts for the Type 1 Audit and 200 artifacts for the Type 2 Audit. Audits were conducted onsite taking five and three days respectively. While the process is certified by AICPAs, at least one of the auditors is an IT/Software security professional with substantial credentials.



Join over six million users in 100+ countries to create your adaptable, everywhere, and connected workspace today.

About Act!

Act! makes it easy to build relationships that last with quick, organized access to highly personalized customer details. Because every business runs differently, you have the freedom to tailor an Act! experience to your business and industry needs—your adaptable, everywhere, connected workspace. Finally, a CRM solution that's uniquely yours.

Call **866-873-2006**
Visit **act.com**



See important details about purchase, system requirements, and add-on products compatibility at act.com/importantnotes.

©2018 Swiftpage ACT! LLC. All rights reserved. Swiftpage, Act!, and the Swiftpage product and service names mentioned herein are registered trademarks or trademarks of Swiftpage ACT! LLC, or its affiliated entities. All other trademarks are property of their respective owners.

621 17th Street, Suite 500 | Denver, CO 80293 | (866) 873-2006 | act.com