SOC Reports: Give Your Customers Confidence in the Services That You Provide to Them

Keiter
Your Opportunity Advisors

April 2013

By Ben Sady, CIA, CISA, CRISC

An entrepreneurial drive for innovation, to create a better product, to solve a problem, leads technology based companies to innovate and find solutions. The process is hard, but rewarding.

If the end product is a business-to-business (B2B) service or business-to-consumer (B2C) service, then there is a strong likelihood that the business is storing, processing, or transmitting data and transactions on behalf of its customer.

To meet the demands of customers, regulators, and the market, most B2B and B2C technology-based companies need to prove that they are protecting customer data and providing quality services.

How are consumers concerned with technology company services?

As B2B and B2C customers get savvy to the risks of sharing sensitive data and outsourcing processes, they are getting more concerned about security, availability, confidentiality, process integrity, and customer privacy. Nobody wants to be responsible for a relationship that leads to data breaches or processing inaccuracies.

Some examples of customer concerns may include the following:

- If your solution is cloud based (e.g. SaaS, PaaS, IaaS), then your customers are likely concerned with security and availability.
- If your solution includes the collection of personally identifiable information, then your customers are likely concerned with customer privacy.
- If your solution is to process transactions accurately, completely, timely, and in accordance with a requirement, then your customers are likely concerned with process integrity.

How can SOC audits provide costumer confidence in technology based services?

The American Institute of Certified Public Accountants (AICPA) has three types of Service Organization Control (SOC) reports to address customer and regulatory needs. Depending on the audit report pursued, these audit reports provide a way for B2B and B2C service providers to demonstrate that they are protecting customer data and providing quality services.

SOC 1 Audit Report (Formerly SAS 70, now SSAE 16) – If a company outsources a process or technology that is material to their financial statements, then the outsourced service provider would normally have a SOC 1 audit performed to provide assurance that controls are in place over the outsourced services that the company provides to its customers.

SOC 2 Audit Report – If a company outsources a process or technology and its customers care about how the outsourced service provider handles security, availability, confidentiality, process integrity, and customer privacy, then the outsourced service provider would normally have a SOC 2 audit performed to provide assurance that controls are in place over the outsourced services that the company provides to its customers.

This report can be provided to customers, regulators, or just be used as an internal tool to demonstrate compliance with best practices. The report is based on the Trust Service Principles and Criteria (TSPC), which include: security, availability, confidentiality, process integrity, and customer privacy. The audit can be completed for one or all of the TSPC and can also be mapped to other standards (e.g. ISO 27002, ISO 15288, NIST 800-53, PCI DSS, HIPAA, GLBA, Cloud Security Alliance's Cloud Controls Matrix, etc.).

SOC 3 Audit Report – This audit is performed for the same reasons and with the same level of rigor as a SOC 2 audit. However, the SOC 3 audit report is considered a general use report and can be widely distributed as a marketing tool.

Because the report can be widely distributed, the SOC 3 audit report is abbreviated and does not include all of the detail that a SOC 2 audit report includes.

What is the benefit of having an SOC audit completed?

In the past, we have outlined the benefits to obtaining SOC audits (see http://keitercpa.com/services/risk-advisory/benefits-of-a-sas-70/). This was written prior to SSAE 16 and uses SAS 70 terminology; however, the principles remain the same. Efficiency and cost reduction, peace of mind, strengthen existing relationships, attract customers, differentiate from competitors, and meet compliance requirements.

As part of a technology-based company's risk assessment process, the company should be assessing whether a SOC audit would be a cost effective tool to pursue and how it would benefit them.

For questions more information regarding SOC audits and reports, please contact Ben Sady at bsady@keitercpa.com.

Stay in touch

Information provided by Keiter is intended for reference only. The information contained herein is designed solely to provide guidance to the reader, and is not intended to be a substitute for the reader seeking personalized professional advice based on specific factual situations. This information does NOT constitute professional accounting, investment, tax or legal advice and should not be interpreted as such.

Although Keiter has made every reasonable effort to ensure that the information provided is accurate, Keiter, and its shareholders, managers and staff, make no warranties, expressed or implied, on the information provided. The reader accepts the information as is and assumes all responsibility for the use of such information. All information contained is protected by copyright and may not be reproduced in any form without the expressed, written consent of Keiter. All rights are reserved.

IRS Circular 230 Disclosure:
To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding any penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction(s) or tax-related matter(s) addressed herein.