AICPA®

Case Study

Putting SOC Reports to Work at Confirmation.com

Service organizations must reassure their users about the safety and integrity of their data while they are at the service organization. One company's experience illustrates the value of SERVICE ORGANIZATION CONTROL℠ Reports and how a service organization can use them.

BACKGROUND

Confirmation.com is a secure, online clearinghouse that provides audit confirmations for entities such as banks and other companies that receive requests for the confirmation of data. It was launched a decade ago by C. Brian Fox, CPA, its founder and chief marketing officer, to bring greater efficiency and security to the existing paper-based confirmation process. Today, the 30-person company processes more than $1 trillion in electronic confirmations annually. Users of its bank confirmation service include each of the top 10 banks in the country and the Federal Reserve. Companies that use the service to confirm trade receivables include Delta, Microsoft, Halliburton, Yum! Brands, the Boy Scouts of America and the American Cancer Society. "There are several hundred thousand companies whose information goes through our systems when their auditors are doing confirmations," Fox says.

AN EXAMPLE

How do organizations use companies like Confirmation.com? As an example, a CPA firm performing an audit of XYZ Company's financial statements sends GreatBank a request for confirmation of XYZ's cash balance. GreatBank (the user entity) uses Confirmation.com (the service organization) to provide confirmation responses to the CPA firm.

As part of that same audit, the CPA firm requests a confirmation from Retail-a-Rama of the amount Retail-a-Rama owes XYZ Company. Retail-a-Rama (the user entity) uses Confirmation.com to confirm the amount that Retail-a-Rama owes XYZ Company.

PROBLEM AND SOLUTION

Given the nature of its service offering, global reach and large volume, high-profile customers, Confirmation.com identified a problem it needed to solve to maintain and grow its business: How can it provide assurance to its users regarding the controls it implements to protect the privacy and confidentiality of users' data as well as the security, availability and processing integrity of the system that generates the confirmations?

In the past, Confirmation.com underwent a Statement on Auditing Standards No. 70 Type 2 examination as well as SysTrust and WebTrust examinations. SAS No. 70 and its replacement, Statement on Standards for Attestation Engagements No. 16, address controls at a service organization that affect user entities' financial statements and are used by CPAs auditing a user entity's financial statements. Recently, the AICPA introduced a family of Service Organization Control Reports (SOC 1℠, SOC 2℠ and SOC 3℠ reports; see next page) that address various types of controls at a service organization.

Confirmation.com has chosen to get all three types of SOC reports because of the broad variety of users of their cloud-based confirmation service and those customers' varying needs. "There are different hot buttons for each organization" that use the services provided by Confirmation.com, Fox notes. In addition to the assurance about controls relevant to users' financial reporting provided by a SOC 1 report, the SOC 2 and SOC 3 reports provide assurance that is important to users regarding the security, availability or processing integrity of a service organization's system and the confidentiality or privacy of the information processed by that system.

This thorough approach also is designed to distinguish the company in the marketplace. Having all of the SOC reports that address all

SOC 1, 2 and 3 Reports: Understanding the Differences

Service Organization Control (SOC) Reports examine controls over the services a service organization provides to users, offering valuable information that users need to assess and address the risks associated with an outsourced task. Three types of SOC reports exist, which are listed on the next page.

five Trust Services principles "gives us a leg up on any potential competition because we have set the bar high and established that we take issues such as privacy and confidentiality seriously," he says. Fox's participation in webcasts and conferences, in which he reviews his company's steps to ensure security, are another way to leverage the SOC reporting process. "I mention the reports in every presentation," he says. Since he believes that an industry-wide high standard is in his own company's best interest, he also wants to set the groundwork for what any other business would need to enter the market. "We want to set a minimum threshold with our service. If another company that provides confirmation services had a breach, it would taint the entire electronic confirmation marketplace, so we want to promote this level of best practices. Since our industry is relatively new, there's a better chance of a breach happening from some new player. We have a higher risk of reputational damage from a bad player in the marketplace."

Among other benefits, Fox says that users will be better able to understand the purpose of each SOC report and the common nomenclature used. "The SAS 70 reports had been misused in the past in ways that went beyond the original intent," he says, leading to confusion about their purpose.

PROCESS

Confirmation.com provides SOC reports every 6 months, each for a 6-month period ending May 31 and Nov. 30. Taking on this challenge "ensures we're constantly thinking about how we can improve our processes," Fox says. "It keeps security, privacy and all the other issues that are important top of mind. Thinking about their importance and ramifications has become part of our DNA, part of our business and the service we provide."

The majority of the company's customers use its SOC 3 reports, which are publicly available on Confirmation.com's website and useful to those with less technical security expertise. "They know to expect our reports, so they'll look for them in the month after they're released when they're updating their files," Fox says. The company provides its SOC 1 and SOC 2 reports to customers who are interested in the additional information and detail provided by these reports.

Confirmation.com's site includes a security and privacy section that features a link to its SOC 3 reports and the means to request SOC 1 and SOC 2 reports for interested users of those reports. It also features the AICPA's SOC logo for service organizations (at right). The company uses all these elements "to let the public know we are diligent," he says. "We want to brag about it."

Because the SOC engagements occur every 6 months, the company approaches them on a rolling basis. "We have the processes and procedures in place," Fox says, "so it just becomes a standard course of business." When it prepared for its first SAS 70, SysTrust and WebTrust reports, the company brought in an auditor as a consultant to provide feedback on needed changes, offering what Fox calls "a state of the union. They helped us critically evaluate our security procedures and documentation." He recommends taking this step well before the actual examination to leave time for any necessary changes.

The process is led by the company's chief technology officer, with different teams responsible for various steps, including a security and privacy subcommittee. Fox advises service organizations to research the process and reach out to other businesses that have been through a SOC engagement. "Our CTO had been through SAS 70 audits in the past with another company, so that helped us understand what we were getting ready for."

CONCLUSION

Fox says that SOC reports give his company a competitive advantage. Given the widespread interest in security, confidentiality and privacy, he thinks SOC reports are filling an important marketplace need. "For us, SOC reports are extremely pertinent because accounting firms rely on our confirmations when performing audits," he says. "We continue to see more people ask for SOC reports by name."

For additional information, visit aicpa.org/SOC for the latest news, logo and usage guidelines, and resources related to the SOC reports.

1 A SOC 1℠ report evaluates controls at a service organization relevant to user entities' financial statements. It is intended to meet the needs of CPAs that audit the user entities' financial statements (user auditors) in evaluating the effect of the controls at the service organization on the user entities' financial statements. Use of these reports is restricted to the management of the service organization, user entities and user auditors.

2 A SOC 2℠ report, which is intended for a broad range of users, covers controls at a service organization relevant to the security, availability or processing integrity of the system the service organization uses to provide services to users as well as the confidentiality and privacy of the information processed by those systems. Use of these reports generally is restricted.

3 A SOC 3℠ report is a simplified version of a SOC 2 report covering the same subject matter. They are general-use reports and can be freely distributed or posted on a website.

12253-312