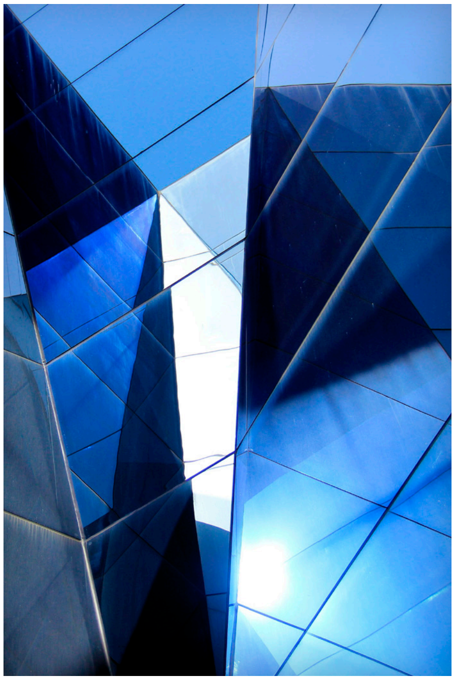
Crowe Horwath®

April 2015

Lessons From the First Three Years of SOC Reporting

Reliance on Third Parties, Rising Security Risks Make Reports More Important Than Ever

By Arshad Ahmed, CISA, CISSP, CPA, Sue Horn, CISA, CPA, and Rod Smith, CISA, CPA



Service Organization Control (SOC) Reports® are used to help organizations assess the control environment at third-party service providers to which they outsource functions like payroll processing, data processing, medical claims processing, and cloud computing. In the three-plus years that organizations have been using SOC reports, a number of trends have emerged that can yield lessons to other organizations. In addition, as the outsourcing of critical functions continues to grow, users of SOC reports need to understand how the reports align with other control frameworks of interest, such as the Cloud Controls Matrix developed by the Cloud Security Alliance and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Three forms of SOC reports address different user organization needs, including internal controls over financial reporting and compliance with Section 404 of the *Sarbanes-Oxley Act* (SOC 1); and internal controls relating to the five Trust Services Principles of the American Institute of Certified Public Accountants (AICPA) – security, availability, processing integrity, confidentiality, and privacy (SOC 2 and SOC 3).

Both SOC 1 and SOC 2 reports are restricted-use reports, meaning that only the organizations that have contracted with the service organization providing services may receive the reports. However, SOC 3, an abridged version of the SOC 2 report, can be provided to other parties for general use.

SOC reports are taking on greater importance as prominent data breaches make headlines around the world and more organizations demand to know how their vendors are protecting the sensitive financial, medical, and personal data entrusted to them. According to recent research on data breaches:

- Forty-three percent of companies had a data breach in the past year.[1]
- Only 15 percent of breaches were reported by the media.[2]
- Between 600 and 700 breaches are reported nationally in an average year.[3]

Many observers expect these numbers are only going to increase, leading to an even greater need for SOC reporting.

Lessons Learned

When assessing the effectiveness of their own SOC reports, service organizations can benefit from the experience of early adopters and perhaps avoid the pitfalls they encountered. Following are several trends that have begun to emerge:

Fewer challenges. As they gain experience issuing SOC reports, service organizations are encountering fewer challenges related to determining the appropriate report type and coverage selections. However, first-year issuers still experience some confusion when determining which principles their SOC 2 reports should cover and defining the scope of their reports. Issuers can reduce the confusion by asking user organizations to identify the concerns they are trying to address through SOC 2 reports. First-year issuers should work closely with their service auditors and user organizations to determine the scope requirements and choose the best report to address those requirements.

Continued improvement. SOC reports reflect continuing improvement in the areas for which service organizations' management is partially or fully responsible. Management assertions are organized more clearly, risk assessments are better documented, and system descriptions are more effective.

Multiple audits. Service organizations are becoming acclimated to SOC examinations because a lot of them are issuing both SOC 1 and SOC 2 reports annually to meet their users' needs. As a result, service organizations are motivated to work with their service auditors to rely on existing internal audit reports, to streamline audits, to minimize disruptions, and to make better use of technology when executing SOC examinations.

Internal audit. As they go through their annual SOC examination cycle, service organizations are able to use the work of their internal audit departments to reduce SOC examination costs and time. For example, internal auditors can provide the service auditor with work papers and supporting documentation from existing audits. The service auditor then can rely on the work performed by the internal auditor.

More user controls. In order for the system of control over the services provided by the service auditor to operate effectively, client organizations are expected to have designed and implemented certain complementary user-entity controls. Management needs to ensure that requisite user-entity controls have been identified, designed, and implemented; and the service auditor must ensure that management has done a sufficient job of identifying and implementing these controls.

Increased interim visits. One of the more beneficial trends in SOC examinations is the increase in interim visits by service auditors, both throughout the attest period and earlier in the audit cycle. Service auditors are required to report all encountered issues as either exceptions or deviations. However, if ineffective controls are corrected early in the audit cycle, they might not have an adverse influence on the audit opinion that is ultimately rendered. By meeting with their clients throughout the year, service auditors can identify and address issues early in the audit cycle.

In summary, service organizations are responding to increased SOC examinations and regulatory requirements by focusing their attention on areas of interest and improving their audit efficiency.

Managing Risk in the Cloud

In recent years, organizations have been outsourcing more of their business services to cloud computing companies – third parties that process and store client data on servers connected to the Internet. According to one recent study, cloud computing services will account for nearly one-fourth of IT budgets in 2015.[4]

In 2010, the Cloud Security Alliance , an international not-for-profit organization that promotes best practices for providing security assurance in cloud computing, introduced the Cloud Controls Matrix (CCM). The CCM helps customers evaluate cloud services providers by using a control framework that aligns with other industry-accepted security standards, regulations, and control frameworks, including SOC reports. Because the attest standards permit extending the trust services principles and criteria to cover other control frameworks, an organization could issue a dual-purpose report that meets both the CCM requirements and the AICPA's Trust Services Principles in a SOC 2 report.

The Future of SOC Reporting

Given the rising threat of third-party risk – and the resulting concerns of boards and audit committees – the demand for SOC reports is likely to continue to increase. While SOC reporting as a whole is growing, demand for SOC 2 reports is increasing at a higher rate than for SOC 1 reports because SOC 2 reports provide assurance beyond controls related to financial reporting.

The heightened demand for SOC reports also means that service organizations likely will need to provide users with both SOC 1 and SOC 2 reports. Organizations are also required to provide assurance that controls are in place to meet other sector-specific risk frameworks. As a result, SOC reports will be used more creatively in the future. SOC 2 reports will evolve in order to demonstrate a service organization's compliance with other control frameworks, such as the *Health Insurance Portability and Accountability Act*, the Payment Card Industry Data Security Standard, the NIST Cybersecurity framework, and additional requirements.

Contact Information

Arshad Ahmed is a partner with Crowe Horwath LLP in the South Bend, Ind., office. He can be reached at 574.236.7602 or arshad.ahmed@crowehorwath.com.

Sue Horn is with Crowe in the Cincinnati office. She can be reached at 614.365.2236 or sue.horn@crowehorwath.com.

Rod Smith is with Crowe in the New York office. He can be reached at 212.751.8151 or rod.smith@crowehorwath.com.

"SOC Lessons Learned and Reporting Changes," a recording of a Dec. 16, 2014, Crowe webinar presentation by Arshad Ahmed, Sue Horn, and Rod Smith, is available at http://www.crowehorwath.com/ContentDetails.aspx?id=10337.

[1] "Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness," Ponemon Institute Research Report sponsored by Experian Data Breach Resolution, September 2014, http://www.ponemon.org/library

[2] Elizabeth Weise, "43% of Companies Had a Breach Last Year," interview with Michael Bruemmer of Experian, USA Today, Sept. 24, 2014, http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/

[3] Ibid.

[4] "IDG Enterprise Cloud Computing Study 2014," IDG Enterprise, November 2014, http://www.idgenterprise.com/report/idg-enterprise-cloud-computing-study-2014; and Louis Columbus, "Cloud Computing Adoption Continues Accelerating in the Enterprise," Forbes, Nov. 22, 2014, http://www.forbes.com/sites/louiscolumbus/2014/11/22/cloud-computing-adoption-continues-accelerating-in-the-enterprise/

Crowe Horwath LLP is an independent member of Crowe Horwath International, a Swiss verein. Each member firm of Crowe Horwath International is a separate and independent legal entity. Crowe Horwath LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Horwath International or any other member of Crowe Horwath International and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe Horwath International or any other Crowe Horwath International member. Accountancy services in Kansas and North Carolina are rendered by Crowe Chizek LLP, which is not a member of Crowe Horwath International. This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction.

RISK15910