Understanding Security Audit Requirements in Technology Contracts

Amanda Witt

Daily Report

August 28, 2015

Many attorneys representing a client who procures technology from a service provider know to request a security audit, but there is still confusion even among sophisticated technology attorneys about which security audit to request and how to interpret the report once it is received.

This article will describe the types of security audits and third-party security certifications that are most frequently requested by customers or offered by vendors. The following types of audit reports and certifications will be examined below:

- SSAE 16 / SOC 1 (formerly SAS 70), Type 1 and 2
- SOC 2, Type 1 and 2
- ISO 27001
- ISO/IEC 27018
- NIST Cybersecurity Framework

While the first Statement on Auditing Procedure was issued in 1949 (according to the web-based SAS 70 History and Timeline site), the popularity of asking a technology vendor for its SAS 70 report can likely be tied to the Sarbanes-Oxley Act of 2002. Because of the accounting fraud of Enron and the assistance provided by its auditing firm in concealing such fraud, Sarbanes-Oxley requires the management of publicly traded companies to certify annually that the company's internal controls in financial reporting were effective.

As part of this annual certification, organizations also examine the controls of their service providers that provide hosting services, transaction processing or other material services in order to evaluate the design and test the operating effectiveness of such third parties' controls. Initially, management of an organization could either conduct these investigations itself or have an auditing firm conduct a SAS 70 Type 2 auditors report.

Over time, the SAS 70 became a tool for organizations to verify the adequacy of a service provider's "security" even though the purpose of the SAS 70 report was not designed to serve this purpose. What many fail to understand as well was that each service provider establishes its own controls, so every SAS 70 is highly customized for each service provider.

When the American Institute of CPAs became aware of the unintended uses of the SAS 70, it created the SSAE 16/ SOC 1 and the SOC 2 report. A SOC 2 report is more narrowly tailored to the services provided by technology vendors. Essentially, the SSAE 16/ SOC 1 should be used when the services provided by a vendor could affect an organization's financial reporting (e.g., the service provider's services include financial-related transactions / processing services) and a SOC 2 should be used when attempting to verify a vendor's controls relevant to security, availability, processing integrity, confidentiality and/or privacy.

The most commonly requested (and offered) report is the American Institute of CPAs' Statement on Standards for Attestation Engagements (SSAE) 16, which is more commonly referred to as a SOC 1 and

replaced the SAS 70. A SSAE / SOC 1 report (and a SOC 2 report) can either be a Type 1 or Type 2 report. A Type 1 report means that the auditor is only providing an opinion as to the design and implementation of the controls on a certain date. A Type 2 report, in contrast, means that the auditor is providing an opinion on the design, implementation and operating effectiveness of the controls (i.e., by testing the controls) over an entire audit period.

Obviously, a customer would be better served by requesting a Type 2 report, but vendors (especially large cloud providers) frequently offer only a Type 1 report. Furthermore, note that a SOC 1 report may deal only with the service provider's controls that are relevant to the customer's financial reporting, so it is likely much narrower in scope than what the customer wants.

If trying to verify the security practices of a cloud vendor, an organization is better served by requesting a SOC 2, Type 2 report. The SOC 2 report examines the service provider's controls relevant to security, availability, processing integrity, confidentiality and/or privacy.

Depending on what services are being provided by a vendor, it is important to identify which controls should be examined (e.g., for a data hosting or cloud provider, security, availability, processing integrity and confidentiality may be the most important). If a customer does not designate which controls are to be tested, the vendor will make the determination. A customer may receive some pushback from the vendor on providing a SOC 2 report because it is more costly than a SOC 1, but it is a more relevant report for a technology-related service provider.

Instead of or in addition to performing a SOC 1 and SOC 2 audit annually, some service providers may prefer to obtain the certification of an independent third party that such service provider's security adequately protects its customers' digital assets. The most common of these types of certifications is the ISO 27000 family of standards, which are designed to assist organizations in securing information assets.

The ISO 27000 family includes two standards: the ISO 27001 standard, titled "Information technology—Security techniques—Information security management systems—Requirements," and the ISO 27002 standard, titled "Information technology—Security techniques—Code of practice for information security controls."

The most common certification in the technology and outsourcing industries is the ISO 27001 certification, which designates an Information Security Management System (ISMS). The ISMS is dynamic and is based on the "Plan-Do-Check-Act" principle, which means that it is designed to be updated regularly in order to address evolving security threats, vulnerabilities and business consequences. As noted in a recent article by Paul de Hert and others in Brussels Privacy Hub, Vol. 1 No. 2, the ISO 27001 standard "lists requirements for the establishment and operation of an ISMS and covers high-level operational and staffing issues." Further, the article noted that the ISO 27002 standard "gives guidance on practices on selection, implementation and management of controls in ISMS [and] … is designed to be used as a reference for selecting controls within the process of operating an ISMS based on the ISO/IEC 27001."

Tied with the rise in popularity of cloud-based services and the looming change in European privacy laws that will make such laws more likely to apply to American companies, ISO and the International Electrotechnical Commission jointly issued the ISO/IEC 27018 standard in July 2014. The new standard is designed to provide guidance that is specific to cloud service providers who process personally identifiable information (PII).

According to de Hert's article, the new standard builds on the ISO 27001 and 27002 standards, which primarily apply to confidentiality, integrity and availability controls, and "focuses on information privacy risks from the perspective of [a] PII processor." The goal of the new standard is to "address the specific risks of public cloud computing and help build confidence in public cloud computing providers while also providing guidance on what cloud providers need to implement in terms of contractual and regulatory obligations."

The most important alternative set of standards to ISO is the National Institute of Standards and Technology Cybersecurity Framework, issued in 2014. Although the NIST Cybersecurity Framework must

be followed by organizations providing services that affect critical infrastructure, the framework is scalable so as to be suitable for organizations securing lower-risk data and systems.

As concerns about the security practices of service providers continue to grow with the occurrence of each high-profile security breach, the reliance on security audits and security certifications will continue to increase steadily. There is significant "security questionnaire fatigue" in the technology industry as customers bombard their service providers with extensive, time-consuming security questionnaires.

The likely solution to the inefficiencies of current practices is some sort of standardization for measuring a service provider's security controls. While ISO/IEC 27018 and the Cloud Security Alliance's STAR may have the potential to fill this need for cloud-based services, a broader standard for all technology-related service providers is not yet available.

Amanda Witt is a partner at Kilpatrick Townsend & Stockton and focuses her practice on complex commercial transactions along with global privacy and information security counseling. She has delivered presentations and published articles on privacy, cloud computing, electronic signatures, security and outsourcing.