New Guidance for Cloud-Based Service Control Reports

An Introduction to AICPA SOC Reports and SSAE 16

By Josef Rashty

When a series of technical problems plagued Amazon.com in April 2011, some customer data were lost as a result of an extended outage in its Amazon Web Services Elastic Compute Cloud (AWS EC2) service. On April 23, the *Wall Street Journal* reported that Google Inc. took an unusual step in response to this incident—it posted a video online demonstrating the steps it has taken to ensure that its data centers are reliable and can protect users' information.

Since their beginning, cloud services have been remarkably reliable, and this track record has fostered a dangerous complacency among customers, who may be putting too much trust in the operations of their system providers. For example, although Amazon has consistently claimed 99.95% out-of-the-box uptime availability, its recent AWS EC2 incident proved that cloud-based computing could potentially pose significant financial and operational risks (John Bair, "On the Reliability of Cloud Computing," BeyeNetwork, April 2011, www.b-eye-network.com/view/15180).

The operation of service providers affects the internal controls related to financial reporting of user entities. Recent AICPA guidance addresses the preparation of different service organization control (SOC) reports, as well as the control environment of cloud-based computing arrangements.

Cloud-Based Computing Arrangements

After IBM unbundled its hardware from its software, it introduced an enterprise software system in 1969—that is, a collection of computer programs for an entire organization rather than just a segment of the enterprise. Enterprise software applications platforms have evolved since then—from mainframe computers to minicomputers, from minicomputers to desktop computers, and from desktop computers to client-server environments. Each platform shifted the focus of the enterprise software applications to a new type of user group, progressing from a centralized IT department to distributed end-users.

The Internet has brought dramatic changes to the software industry in the past 20 years, including the introduction of open standards, a nonproprietary protocol or specification governed by an organization open to all who wish to join, such as ISO standards; the development of open source, software whose source code is made available for use or modification as users or other developers see fit; and finally, cloud-based computing environments.

An enterprise computer system requires users to pay for a set of computer resources, consisting of software and hardware, based on their peak needs. Furthermore, the installation of an enterprise computer system is often a very lengthy and expensive process, both in terms of resources needed and upfront cash outlay. In response to such perennial problems, cloud computing applications have recently gained popularity. Cloud computing is an Internet-based and on-demand system that provides virtually unlimited,

variable computing resources at a reasonable cost. Cloud computing, unlike enterprise systems, can deploy technology solutions in a matter of days, rather than months or years.

The National Institute of Standards and Technology, an agency of the Department of Commerce, defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Many companies have embraced cloud-based computing as the current technological paradigm. The term "cloud" is a metaphor for the Internet, and thus cloud computing means that software and data are hosted remotely accessed by users via the Internet. There are several cloud-based services: software-as-a-service (SaaS), a delivery model in which software and its associated data are hosted centrally, typically in the Internet or cloud (e.g., NetSuite); platform-as-a-service (PaaS), the delivery of a computing platform as a service facilitating deployment of applications without the cost and complexity of buying and managing the underlying hardware and software (e.g., Salesforce.com); and infrastructure-as-a-service (IaaS), a combination of hosting, hardware, provisioning, and the basic services needed to run a cloud (e.g., Amazon Web Services).

These services all have three distinct characteristics that differentiate them from traditional hosting environments. First, they are sold on demand, typically by the minute or the hour. Second, they are elastic, and users can have as much or as little of a service as they want at any given time. Third, because they are fully managed by a third-party provider, the consumer needs nothing but a personal computer and Internet access.

Cloud-based products usually include a combination of offerings, such as software, hosting and support, professional services for implementation, and ongoing post-contract support and training. Users consume cloud-based systems on a scalable "as needed" basis and payment arrangements vary; some reimburse the vendors a flat fee for the resources while others pay on the basis of traffic and CPU time utilized. Since vendors offer cloud-based computing systems through the Internet, there is usually no need for customers to install and manage third-party software, related hardware, or networking equipment in-house.

The Control Environment of Cloud-Based Service Organizations

A company's internal controls over financial reporting (ICFR) is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with U.S. GAAP and the standards as set forth in the Sarbanes-Oxley Act of 2002 (SOX) and issued by the Public Company Accounting Oversight Board (PCAOB).

SOX section 404(a) requires that management assess and report on the effectiveness of ICFR as of the end of each fiscal year. Reports on the effectiveness of internal controls are audited at the end of each fiscal year (SOX section 404[b]) based on certain control criteria established in a recognized framework, such as the Internal Control–Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

PCAOB Auditing Standard 5 (AS 5) establishes requirements and provides direction that applies when an auditor is engaged to perform an audit of management's assessment of the effectiveness of ICFR. An effective ICFR provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external users. If one or more material weaknesses exist, the company's ICFR cannot be considered effective. The auditor's objective is to express an opinion on the effectiveness of the company's internal control over financial reporting.

In cloud-based arrangements, an entity outsources a business task or a function to another entity (usually one that specializes in that task or function), and the data that result are incorporated in the outsourcer's financial statements. As a result, the internal controls that should be exercised over financial reporting function reside outside the entity, rather than within the control of management. Nevertheless, the management of the outsourced function remains responsible for the ICFR of the organization as a whole. In these circumstances, a company that has outsourced a service function will most likely request an ICFR service auditor's report from the provider organization, as promulgated under Statement on Standards for Attestation Engagements (SSAE) 16, *Reporting on Controls at a Service Organization* (previously known as a Statement on Auditing Standards [SAS] 70 report).

A company that has outsourced a service function will most likely request an ICFR service auditor's report from the provider organization.

Service Organization Control Reports

The AICPA has developed guidance in the form of service organization control (SOC) reports for providing a highly specialized examination of a service organization's internal controls. These SOC reports are internal control reports that relate information about the services provided by an organization so that users can assess and address the risks associated with outsourced service. These reports are intended for a broad range of users who need to understand the internal controls of a service organization as they relate to the security, availability, processing integrity, confidentiality, and privacy of their outsourced operations.

There are three types of SOC reports:

- SOC 1 reports cover the controls at a service organization relevant to a user entity's ICFR. These reports—prepared in accordance with SSAE 16—are specifically intended to meet the needs of a user entity's financial management and auditor. They evaluate the effect of the controls at the service organization on the user entity's financial statement assertions.
- SOC 2 reports encompass controls at a service organization relevant to security, availability, processing integrity, confiden-

tiality, or privacy. These reports are intended for users who have a thorough understanding of the service organization and its internal controls. A SOC 2 report is an important part of a user's oversight of a service organization.

■ SOC 3 reports, or trusted services reports, are also commonly referred to as SysTrust reports ("Trust Services Principles, Criteria, and Illustrations," AICPA, Technical Practice Aids, vol. 1, sec. 100). These reports are designed to meet the needs of users who want assurance about the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not need the level of detail provided in a SOC 2 report.

A SOC 1 report is applicable when an entity engages a service organization to perform key processes or functions. Under such circumstances, the user entity exposes itself to additional risks related to the service organization's system. Although an entity's management can delegate certain tasks or functions to a service organization, the responsibility for the proper execution of those tasks and functions cannot be delegated and remains with management. SOC 1 has been issued in response to this need. SSAE 16 does not apply to examinations of controls over subject matter other than financial reporting.

The increasing use of cloud computing services—which provide user entities with on-demand network access to a shared pool of computing resources, such as networks, servers, storage, applications, and services—has created a growing demand for CPAs to report on the nonfinancial reporting controls implemented by cloud computing service providers. SOC 2 reports came about to satisfy this demand for reporting on nonfinancial controls.

When a user entity evaluates controls of a service organization that may be relevant and may affect the services that it receives, management may ask the service organization for a SOC 2 report on the design and operating effectiveness of controls over the service organization's system, which may be relevant to the security, availability, or processing integrity of the system, as well as the confidentiality or privacy of the information processed for the user entity.

SOC 3 reports are typically general-use reports and can be freely distributed to any interested third party or be posted by the service organization on its website as a seal of approval.

Exhibit 1 summarizes the features of these three reports.

SSAE 16 Requirements

The AICPA issued SAS 70, *Service Organizations*, in April 1992. It acted as the governing standard for performing such audits prior to the issuance of SSAE 16 and served as an assessment of the ICFR of the service organization for the customer and the customer's auditor. The requirements of SOX section 404 made SAS 70 audit reports even more important to the process of reporting on the effectiveness of ICFR.

In April 2010, the AICPA's Auditing Standards Board (ASB) issued SSAE 16, effective for reports with periods ending on or after June 15, 2011. Although SSAE 16 does not represent a significant change from SAS 70, service organizations must still be prepared to meet new levels of trust and transparency under the standard. The counterpart to SSAE 16 is International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, which is also effective from June 15, 2011.

Generally, the primary focus of SAS 70 is to provide guidance for reporting on audits of financial statements, whereas SSAE 16 provides guidance for reporting on other subject matters as well. Otherwise, SAS 70 and SSAE 16 are substantially the same, except for one main difference: SAS 70 is an audit standard while SSAE 16 is an attest standard. A provision to require a written assertion from company management is the most notable substantive difference between the two standards.

SSAE 16 requires that the service organization provide a written assertion about the types of transactions and processes covered under the report. In this assertion, management communicates to customers and to others that the system of controls is fairly presented and is designed and operates effectively. In addition to this assertion, management must prepare a description of the service organization's system, which should include all of its policies and procedures, as well as controls surrounding the service processes. This description must include any risk assessment process and monitoring of controls—as defined by COSO's internal control framework—that might be relevant to user entities.

Management's description of the system should identify risks and those controls that could potentially mitigate them. Organizations that have formal risk assessment processes in place, as part of a SOX section 404 compliance program, may find the concepts and principles of SOX section 404 applicable to SSAE 16 requirements. Management's description of the service

EXHIBIT 1
Summary of SOC Reports

Type of Report	Users	Reason	Scope and Purpose
SOC 1	Controller's office and user's auditor	SOX section 404	ICFR
SOC 2	Other non-financial users and regulators	Oversight and due diligence	Security, availability, confidentiality, processing integrity, and privacy
SOC 3	Any user or interested party public	Marketing	Organization's seal of approval and easy-to-read report

organization system should also clearly distinguish the services that a subservice organization provides to its customers and explain the controls in the subservice organizations, if they exist, as well as how they are related to the ICFR of the customer.

SSAE 16 offers an expanded definition of internal audit that includes members of the compliance or risk departments who perform duties similar to the internal audit (such as SOX section 404 compliance testing). Service auditors may use the work of internal audit or other control-related functions that has been performed independently of the service auditor's work to support their testing. In such a case, the service auditors should disclose the reliance on the work for their reports.

There are two types of service auditor's reports based on SSAE 16. In both reports, the service organization must prepare a description of its system that includes, among other things, the nature of the service provided, how the service is performed, and the service organization's controls over the service and related control objectives. In a type 1 report, the service auditor expresses an opinion on whether the description is fairly presented (i.e., does it describe what actually exists?), whether the controls included in the description are suitability designed, and whether these controls are able to achieve the related control objectives if they operate effectively. In a type 2 report, the service auditor's report contains the same opinions that are included in a type 1 report, plus an opinion on whether the controls were in fact operating effectively.

An Active Approach

Several recent internal control breakdowns in the service organizations have increased the focus of management and auditors to matters other than financial controls. This change of focus has resulted in an increased demand for attestation on subject matter other than financial reporting. The recently issued SSAE 16 can help an entity's management and auditors evaluate the financial effects of controls at service organizations. But neither SSAE 16 nor the earlier SAS 70 addresses controls over subject matter other than financial reporting. In response to this demand, AICPA developed the SOC reporting framework. SOC 2 and SOC 3 reports provide auditors with the opportunity to expand their attestation function to subject matters other than financial reporting.

A company cannot simply adopt a hands-off approach when it comes to monitoring the control environment of service providers in cloud-based computing arrangements. Businesses increasingly need to obtain more information about the operations of service providers and to more carefully scrutinize service providers' methods for handling potential problems. ❑

Josef Rashty, CPA, *has held managerial positions with several publicly held technology companies in the Silicon Valley region of California. He can be reached at jrashty@sfsu.edu.*