INTERNAL CONTROL OVER FINANCIAL REPORTING AND THE CLOUD

I. Hilmi Elifoglu, St. John’s University, USA

Yıldız Guzey, Beykent University, Turkey

Özlem Tasseven, Doğuş University, Turkey

Abstract:

By 2020, 40 percent of digital information is expected to be created in the Cloud, delivered to the Cloud, or stored and manipulated in the Cloud. It is clear that the Cloud is here to stay.

As a large scale version of outsourcing Cloud Computing will create new challenges and complications for management and auditors. After the replacement of SAS 70 with SSAE 16, (similar to the ISAE 3402), most Cloud Service Providers will provide assurances to the Cloud Service Users within the framework of attestation standards instead of auditing standards.

Outsourcing presents some challenges in itself and cloud computing further complicates those challenges. The new framework allows three different deployment models in the form of SOC1, SOC2 and SOC3. It is crucial that cloud service providers and cloud service users and their auditors should carefully consider alternative Service Organization Controls (SOC) deployment models. Unfortunately, many cloud providers are opting out for SOC 1 leaving little room for the development of SOC 2 reports. The right SOC deployment model for the Cloud is SOC 2 or SOC 3.

I. THE CLOUD DEFINED

To clarify the concept we will employ the definition provided by National Institute of Standards and Technology (NIST):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

In this definition, the Cloud is shown as a product of the convergence of the Internet technologies with virtualization, and IT standardization. In this environment the most common characteristics are:

- **Broad-band access and location independence:** The system can be reached via the Internet from any computer using a standard browser from anywhere at any time. The user does not need to know the location of the system.
- **Pay as you use for a measured service and scalability:** Since there is no initial investment in hardware and software, most subscribers see only the variable cost of computing. You pay only for what you use. Metering is a must. The resources are easily scaled and can be automatically adjusted to meet demand without any human
intervention. The infrastructure can be easily resized and right sized, depending upon need.

- **Full customer self-service:** Customers can subscribe, manage, and terminate services themselves without any human intervention with ease. Instead of days or weeks, the time dimension is measured in hours.

- **Resource Pooling (Multi Tenancy):** The service provider’s resources are pooled to serve multiple users (tenants) simultaneously. Different physical and virtual resources dynamically assigned and reassigned according to user demand.

The Cloud computing can be provided with three service models, four deployment models.

**a) Service Delivery Models:**

Cloud computing services are delivered in three distinct formats: **SaaS (Software as a Service)**, **PaaS (Platform as a Service)**, and **IaaS (Infrastructure as a Service)**.

Typical SaaS provides online processing or data storage capacity. Application resides on the provider’s computers with very little customization. User organizations do not maintain technical staff as we see in Salesforce.com, Oracle on demand, Myerp.com and Facebook.

The PaaS structure provides a platform and tools for developing and hosting other applications, such as database services. Users obtain an easy access to programming languages and tools offered by the provider. The users still maintain a portion of their own technical staff to write their own code.

The IaaS provider maintains infrastructure in the form of servers, operating systems, networks, storage devices and databases. This model is highly virtualized and requires minimal configurations for customization as we see at Amazon EC2, Rackspace and Mozy.com

**b) Deployment Models:**

The Cloud may be deployed as **private or public**. When dedicated to a single enterprise, they are known as “Private Cloud”. Enterprises using private clouds will continue to incur capital expenditures depreciated over time. When resources are shared with other enterprises, they are known as “Public Cloud”. From the subscriber’s point of view, the public cloud is owned and managed by a third party. By avoiding the initial investments in hardware and software, the public cloud minimizes cash out-flow for the user organization. In the public cloud alternative, the user organization no longer has direct control over its own data even though the user organization still remains responsible for compliance with all applicable laws and regulations. Examples include Amazon’s Elastic Cloud (EC2), Sales Force and Gmail.

In some cloud deployment models, the public and private cloud infrastructure is combined. In **Hybrid Cloud** deployment models, the private cloud is allowed to access public cloud during the peak periods when the private infrastructure cannot answer the computing requirements (called cloud bursting). In **Community Cloud** deployment model, several organizations with similar
missions, objectives, security requirements and compliance needs share the same cloud infrastructure.

c) Standard Setters for the Cloud

The Cloud standards and related regulations are still evolving. The following are the most prominent regulators and standard setters in this field.

- **CSA (Cloud Security Alliance):** Non-profit consortium to promote the use of best practices for providing security assurance and education on the use of Cloud computing.

- **ENISA (European Network and Information Security Agency):** ENISA works with European Union countries on Cloud security issues.

- **ISACA (Information System Audit and Control Association):** A pace-setting global organization for information governance, control, security and audit professionals.

- **NIST (National Institute of Standards and Technology):** NIST tries to facilitate the development of standards for better collaboration in the information technology field.

- **FedRAMP (Federal Risk and Authorization Management Program):** A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

II. THE CLOUD AND THE AUDITING INDUSTRY

Before 2011, the Cloud had been considered as a special case of outsourced IT operations by AICPA. In a typical outsourcing the service user entity engaged a service organization to perform some of the business processes or functions on its behalf. However, the transferring out the services does not change the accountability of the service user. The accountability remains with the service user. The auditor of the service user needs assurances about the controls at the service provider.

Since its release in 1992, SAS-70 provided the necessary guidance to CPAs who audit the financial statements in outsourcing environments. The original purpose of the SAS 70 was a report to be used between the auditors of service users and service providers. SAS 70, has been assumed to provide enough guidance for CPAs reporting on internal controls at service organizations. However, the compliance requirements of the Sarbanes-Oxley Act and the PCAOB’s AS5 led to a wider use of SAS 70 at the global level at the global level. Many service users started requiring more evidence on the design and operation of controls from the service providers to ensure that the user entity’s control requirements have been met.

Even though the principal goal of the SAS 70 was the reliability of the financial statements, “SAS 70 like control reports” have become increasingly widespread in the United States and
around the world to meet the requirements of various regulatory agencies and governmental entities. Some of the SAS 70 audits covered issues like logical and physical access to information, organizational controls, application development and maintenance controls, data processing controls and business continuity controls.

Since most of the “SAS 70 like reports” went beyond the traditional financial statement audits and addressed issues traditionally related to the Trust Services principles of AICPA, in 2011, the Auditing Standards Board (ASB) has replaced SAS 70 with a new attestation standard, SSAE 16, “Reporting on Controls at a Service Organizations” to deal with some of the Cloud specific issues. The new standard, also in accordance with the ISAE 3402 of the International Auditing and Assurance Standards Board (IAASB), allows the employment of three Service Organization Control (SOC) reports -SOC 1, SOC2, and SOC3 in Type I and Type II formats. For practical purposes, because of close cooperation between the two organizations, there are insignificant differences between SSAE 16 and ISAE 3402.

I. Type I and Type II Reports

Under SSAE 16, just like SAS 70, the service auditor can issue either Type I or Type II reports. A Type I Report includes management’s description of a service organization’s system and the suitability of the design of controls at a given moment in time. A Type I report does not deal with the effectiveness of the controls. On the other hand, the Type II report deals with the design and operating effectiveness of controls for a time period, such as a year or quarter. Because of its scope, the Type II report is usually preferred.

Under SAS 70, it was the auditors who reported directly on the controls. This was a communication between the auditors involved. The management of the service provider was not required to attest to anything. Under SSAE 16, the management of the service provider is required to prepare a written assertion attesting to the fair presentation and design of controls.

II. SOC 1, SOC2 and SOC 3 Reports

Under SSAE 16, the auditor’s task is essentially to issue a report, called Service Organization Control (SOC) on the design and description of controls that may be relevant to the user entities’ needs. The SOC reports may be in three distinct forms -SOC 1, SOC 2, and SOC 3. Each one of these reports may be combined with Type I or Type II reports.

i) SOC 1 Reports: The SOC 1 Report is prepared in accordance with AT 801 by an independent service auditor. SOC1 reports require a detailed description of the service organization’s controls that are likely to be relevant to a user entity’s internal control over financial reporting (ICFR) system along with a written assertion by management. SOC1 framework places greater emphasis on the ICFR component for service organization than SAS 70. The SOC1 report requires that the risks related to the financial
reporting processes are adequately addressed. Service organizations, such as payroll processing, and medical claim processing, which initiate and process a business processes from beginning to the end are the best candidates for SOC 1 reports.

ii) **SOC 2 Reports:** The SOC 2 and SOC 3 reports, based on AT Section 101, Attestation Engagement, go beyond the financial reporting assurances of SOC 1 reports.

The SOC 2 reports are designed to deal with issues uniquely related to ever expanding computer based service entities, such as data centers and cloud computing. For instance, an entity providing on-line admission services for a university has to provide assurances to the service user (university) on the privacy and confidentiality of personal information collected. In this instance, there is no direct link to the financial statements (i.e. ICFR).

The SOC 2 reports, issued by the service organization’s auditor, provide assurances about Security, Availability, Processing Integrity, Confidentiality and Privacy to the users of the service. In a type II-SOC 2 report, a description of the service auditor’s tests of controls and the results of the tests will be reported. For instance, in a type II-SOC 2 report that addresses the privacy concerns, a description of the service auditor’s tests on privacy or security and the results of those tests should be listed.

The following is the principal components of a Type II SOC 2 report for a typical service provider:

- *Description* of the service organization’s system by the management of the service provider.
- *Written assertion* by the service provider’s management on security, availability, processing integrity, confidentiality and privacy controls are fairly presented and suitably designed and operating effectively.
- *Service auditor’s opinion* of the fairness of the description of service organization’s system, the suitability of the design of the controls to achieve specified control objectives, and in a Type 2 report, the operating effectiveness of those controls.
- In a Type II report, a description of the service auditor’s *tests of the controls with their results* will be added.

iii) **SOC3 Reports:** SOC2 reports can be distributed to any user entity. The SOC2 report is not distributed to other users, such as sub-vendors without the permission of service organization. On the other hand, a SOC 3 report is a general-use report and can be freely distributed. In contrast to SOC 1 and SOC 2 where there is a Type I option, a SOC 3 report is performed as a Type II only. A SOC 3 report provides only the auditor's report on whether the system achieved the trust services criteria. There is no description of tests and results or opinion on the description of the system SOC 3 report. Typically, the entity will be allowed to place a seal on their website upon successful completion.
III. QUESTIONS FOR THE CLOUD USER AUDITOR

As stated above, the SOC 2 report focuses on non-financial controls as they relate to confidentiality, integrity and availability. On the other hand, the SOC 1 focuses on financial reporting controls.

During the first year of the implementation of SSAE 16, we have witnessed some Cloud providers opting out for SOC 1 in place of SOC 2. There was a noticeable hesitation in the issuance of a SOC 2 reports in the Cloud sector, as seen in the example of Google’s app engine. When a well-known cloud provider like Google provided assurances in a technically incorrect SOC 1 framework, there were doubts about the implementation of the SOC reports. Currently, many assurances in the Cloud sector, including Google, are in the form of Type II – SOC2 reports.

Regardless of the reporting framework, because of the complicated nature of the Cloud service delivery and deployment combinations, the auditor in a Cloud environment should go beyond the traditional service level agreements (SLA). The following are some of the Cloud specific questions that should be addressed by the Cloud user’s auditors:

• **International Dimension and Privacy:** Since the public cloud has no national borders, the corporate data may reside in other countries with different rules and regulations about the organizational data. The privacy rules of one country do not apply uniformly across the globe. How can the Cloud user ensure compliance with laws prohibiting data from being stored in certain countries? How can we assure the privacy of the organizational data in another country?

• **Security Breaches:** One of the most common things in the digital world is the security breaches. How will the cloud provider identify, respond to, correct, and disclose data or other security incidents that negatively affect the user company and its customers? What are the user organization’s audit rights for data loss or data breach?

• **Privacy and Encryption:** Who can access the user data when it is at rest or in transit on a provider platform? What type and level of encryption is employed while the data is in transit or at rest? Who controls the encryption key? What is the location of the encryption key? What types of controls or procedures are in place to restrict privileged users within the cloud from viewing or modifying the sensitive data stored in the provider’s infrastructure?

• **Audit Rights, Integrity and Availability:** To remain in compliance with Section 404 of the Sarbanes Oxley Act, the auditors for the user organization must be able to vouch for the integrity and availability of any company data residing in the public cloud. What are the audit rights (or forensic privileges) for the user organization? What rights does the user organization have in case of forensic investigations? In a multi-tenant environment, what
measures are employed by the provider to segregate the client’s data from the data of other clients? In a multi-tenancy case, how does the provider secures the media access control (MAC), and the IP addresses from the other users? Recovery time objective and back up frequency should be consistent with the enterprise security policy.

- **Exit Strategy**: It may not be frequent but some Cloud providers will go out of business as the competition intensifies in the industry. Moving from one cloud provider to another will be close to impossible because of compatibility related issues in data, program and operating system differences. In the event of a contract termination, the disclosure of programs and data on the Cloud servers may create opportunities to attack the user. Therefore, Cloud service provider must wipe out the user data permanently.

Here is an additional list of other factors the Cloud user and its auditor should consider for an exit strategy should the service provider fails to deliver on its SLA because of

- changes in price, or
- changes in ownership, or
- bankruptcy, or
- soured relationships, or
- data security or privacy breaches, or
- fall behind its competitors, or
- prolonged outages

**IV. CONCLUSION**

As a new form of outsourcing the Cloud is here to stay because of the economic advantages it provides to the user. However, there are significant risks associated in the audit of the Cloud. Most of those risks are related to the hardware, software and infrastructure of the Cloud. From a financial reporting point of view, a Type II- SOC 1 report would be considered sufficient for many outsourcing engagements based on the assumption of independence of the computer system from the financial information.

The same cannot be said for the Cloud because of its dependency on the computer technology. In a Cloud arrangement, the risks associated with the computer technology are an integral part of the financial reporting risks. The server, the operating system, the programs and the data are not visible to the auditor of the Cloud user. Any failure in the Cloud hardware and software will lead to a financial reporting problem. In the Cloud, it is impossible to think of a computer risk independent of the financial reporting risk.

Therefore, an assurance that deals with the Cloud system as whole is needed. For this purpose a type II- SOC 2 report for the Cloud provides the highest level of assurances for confidentiality, integrity and availability. As the popularity of the Cloud increases, we expect to see more type II-SOC2 reports.
End Notes

1 http://idcdocserv.com/1414
2 http://www.ssa16.org/white-papers/soc-1-vs-soc-2.html
3 National Institute of Standards and Technology Special Publication 800-145 (January 2011)
4 www.cloudsecurityalliance.org
5 www.enisa.europa.eu
6 www.isaca.org
7 www.nist.gov
8 http://www.gsa.gov/portal/category/102371
9 Listed below are a sample of industries and business sectors that have undergone SAS 70 reporting: Credit Card Processing Platforms, Internet Service Providers (ISP), Web Design and Development, Web Hosting, Social Media, Data Centers, Medical Billing, Print and Mail Delivery, Online Fulfillment, Rebate Processing, Transportation Services, Payroll Services.
10 An entity’s internal control and the impact a service organization may have on the entity’s control environment has been an important issue for AICPA, e.g. SAS 44 (December 1982) “Special Purpose Reports on Internal Control at Service Organizations”, and SAS 94 (May 2001) “The Effect of Information Technology on the Auditor’s Consideration of Internal Control in Financial Statement Audit”.
11 Over the years, user organizations started requesting “SAS 70-Like” reports that address more than just their financial reporting controls. For instance, a service user organization in health sector would like to assess the provider organization’s ability to comply with U.S. Health Insurance and Accountability Act (HIPAA). Clearly, this compliance related request is not directly related to the financial reporting.
12 Trust Services principles and criteria are issued by AICPA and the Canadian Institute of Chartered Accounts (CICA). Typical trust services engagement deal with security, availability, processing integrity, confidentiality or privacy concerns. http://www.aicpa.org/interestareas/informationtechnology/resources/trustservices/pages/default.aspx
13 In an attestation engagement, the CPA reports on the reliability of information or an assertion made by another party.
From a practical point of view there are no significant differences in both attestation standards.

The written assertion was not required by SAS 70.

Security – The system is protected against unauthorized access (both physical and logical).

Availability – The system is available for operation and use as committed or agreed upon.

Processing Integrity – System processing is complete, accurate, timely, and authorized.

Confidentiality – Information designated as confidential is protected as committed or agreed upon.

Privacy – Personal information is collected, used, retained, disclosed, and/or destroyed in accordance with established standards.

SOC 3 reports can be issued on one or multiple Trust Services principles, which are security, availability, processing integrity, confidentiality and privacy.

http://www.ifac.org/auditing-assurance


http://aws.amazon.com/compliance/soc-faqs/