Cloud Computing

Cloud computing is becoming an important IT strategy for entities that need varying levels of IT resources and for whom purchasing and maintaining sophisticated and costly IT resources is not an effective strategy. The move to cloud services, however, presents challenges and risks that may impact the IT environments of our audit clients.

Although some of the services associated with “cloud computing” have been used historically by some entities, cloud service offerings are evolving to areas with a greater likelihood of relevance to the audit. The following are example characteristics of cloud computing service offerings that could affect our audits:

- Cloud services are easily changeable and may result in significant changes to the entity’s business processes and internal control over financial reporting during the reporting period.
- Cloud services typically are cost effective, readily available, and easily deployed throughout an entity. This may result in cloud environments being implemented with minimal involvement of, or control by, the entity’s IT department and thus not subject to the entity’s existing IT governance model and General IT Control (GITC) environment.
- Arrangements between the entity and cloud service organizations may be complex and involve multiple third-party providers. Furthermore, the entity may have less visibility about how the cloud service organization manages the service. Cloud service organizations may use other subservice organizations.
- Software applications and data are easily transportable when using cloud services and may move back and forth among the cloud service organization’s own environment and those of any number of subservice providers that the service organization chooses to use. Entities may have no control over or knowledge of either the use of subservice providers or the exact location of the provided resources. As such, throughout the financial reporting period, data and applications may not be associated with a specific IT environment or may be associated with different IT environments on different days making it more difficult to track controls relevant to events and transactions.

These factors pose unique risks to an entity’s IT environment, which can impact the controls an entity must modify or implement in order to manage those risks.

Internal Control over Financial Reporting Implications

As entities take advantage of cloud service offerings, there may be significant changes to business and IT processes that may have a significant effect on internal control over financial reporting.

With the rapid deployment capability of cloud computing services, consideration of the impact on change management is important. The effects of cloud computing on internal controls are often overlooked by the entity when it is relatively easy to deploy or modify an application in the cloud, and especially when the cloud services are procured and implemented outside of the entity’s IT department. Given the potentially significant changes described above, it is important for auditors and management to collaborate in identifying internal control over financial reporting implications related to the entity’s plans for implementing cloud services.

Below are potential areas relevant to the audit, which may be impacted by a planned cloud implementation:

- The introduction of new technologies, architectures, and systems or organizational restructuring often requires a company to reorganize its databases and transfer data from “old” applications to the “new” cloud environment.
or reorganize data in an existing application. A critical aspect is the complete and accurate migration of all data such that no data are lost, placed in the wrong location, or altered in the course of the migration process.

- The engagement team may consider system changes that not only impact the software but also process level activities, such as the impact to automated application and manual controls; data conversion; program development methodology; and GITCs. The technology associated with cloud services may seem to simplify the management of IT from the viewpoint of the entity, but it actually adds complexity to change management and configuration controls and can impact data integrity.

- Changes to interfaces and new interfaces may need to be evaluated as part of the program change element of GITCs.

- Revised or additional monitoring or risk assessment controls may be necessary as a result of the aforementioned changes.

As entities transform their business operations by shifting data, applications, and business processes to the cloud, the management and control of IT resources may change. New challenges will emerge over understanding the flow of information and risks in the entity’s financial information systems.

**Service Organizations**

For entities using cloud computing, there likely will be an increase in the number of service organizations and subservice organizations, and there may be an increase in the number of service organizations that are relevant to the audit.

Cloud computing represents the concept of third-party control of hardware, software, and processes in a manner that may differ from a traditional service organization, since the cloud computing service organization may locate people and technologies using different structures in differing parts of the world that are tied together by the Internet. Such service organizations may operate cloud computing in a continually evolving manner, changing technologies, people, locations, and subservice organizations without notice to the user entity. The user entity may not be aware of the service structure or even the physical locations of the service organization.

**Subservice Organizations**

Engagement teams may consider whether subservice organizations are relevant to the cloud service provider service organization. It is common for there to be multiple organizations (subservice organizations) involved in providing the cloud service provider’s service solution and the engagement team may consider the need to obtain the subservice organization’s SAS 70 (SOC 1) report(s).

An example of multiple cloud service providers organized to provide one cloud service solution is where one or more organizations provide software application services and the software applications are hosted on another provider’s infrastructure, and all or part of the infrastructure may be housed in yet another provider’s data center.
Mapping the Audit Impact of Cloud Computing

Areas of importance and key questions

**Cloud services ecosystem**
- Are any third-party vendors involved which could potentially impact compliance?
- What is the third-party vendor’s role?
- What is the relationship between the primary cloud service provider and the third party?
- What level of assurance does the third party offer the primary cloud service provider?
- Is this level of assurance sufficient to achieve and maintain compliance?
- How is the entire cloud system monitored in terms of compliance?

**Public cloud**
- To what level/degree are the IT services shared with other customers (facilities, network, hardware, software, and support staff)?
- To what level/degree are the IT services standardized; what is the IT services customization potential?
- How does the provider support forensic analysis by independent researchers?

**Certifications**
- What assurance and quality statements can the provider offer?
- Which frameworks are used?
- Which audit tools and methods are used?
- Are all risk areas covered by the controls?
- What is the validity/acceptance of the frameworks used?
- What are the intervals for (re)certification?
- Are the current certifications up-to-date?
- What are the provider’s current deficiencies and issues and what is the status of the follow-ups?

**Regulatory compliance**
- Data privacy directive
- Basel
- Solvency
- SOX
- PCI DSS

**Trends and changes**
- What current initiatives are under way and what changes can be expected?
- What are the political fields of influence?
- How do other organizations cope with rules and regulations?

**License to operate**
- Which (local, international) laws, rules, and directives apply to the customer organization?
- Which IT services are in scope of regulatory compliance?
- What is the current level of compliance?
Data center

Data location
- Where is the customer’s data stored, processed, and archived?
- How is the customer’s data isolated and separated from other customer data?
- Within which jurisdiction does the provider and its data center fall?
- What are the data deletion/destruction policies after termination of the contract?

External private cloud
- To what level/degree are the IT services dedicated to customer (facilities, network, hardware, software, support staff)?
- To what extent can the IT environment be audited by the customer (right to audit)?

Network resilience
- What degree of assurance does the network offer in terms of availability and performance?
- What security mechanisms are applied to the network(s)?
- What is the relationship between the cloud service provider(s) and the network provider(s)?

Security and performance
- Security standards
- Business continuity
- Service availability
- SLAs

Data protection and business continuity
- What is the criticality of the business data?
- What are the organization’s principles, requirements, and expected levels regarding IT services?
- What are the minimum measures and controls which must be in place?
Additional Questions Related to Cloud Computing

Governance
- Have all cloud computing services used throughout the organization been identified?
- What process exists to identify cloud services being used throughout the organization, including cloud services provided by service organizations?
- Does this process include monitoring existing arrangements with service organizations to identify significant changes to provided services, including the introduction of cloud computing services?
- What governance process has been implemented to ensure that only authorized personnel are able to enter into arrangements with a service organization given that cloud services may be procured outside the IT department, rapidly and often without internal technology investment and deployment?
- Is there a governance model that considers the decisions to be made and controls to be put in place for cloud enablement of business processes?
- Given that cloud service organizations may store the entity’s data in data centers located in various jurisdictions around the world, has the entity considered compliance with local laws and regulations restricting the transfer of information across borders? Is data able to be obtained and recovered in a timely manner?

Risk Management
- Have the risks associated with cloud computing arrangements been evaluated by management, including the entity’s Internal Audit department?
- Has the impact of the use of cloud service providers on the adequacy of monitoring and risk assessment controls been evaluated, and have new or revised controls been implemented as necessary?

Information Security
- Is there an understanding of how the service organization uses, retains, and discloses personally identifiable information and other highly confidential information given that the entity’s data, and the systems processing the data, may move from data center to data center around the world without the knowledge of the entity?
- Will access to the cloud-based application be integrated with internal systems and therefore use internal logical access controls or be part of the cloud service provider’s logical access controls?
- What changes will be made to access the programs and data controls both internally and at the service provider? For example, who will be granted super-user access? Will other third parties be granted access? How will user access be administered and will the cloud service provider provide security monitoring over logging and monitoring of access, including timely discovery, assessment, and reporting of breaches?

IT Management
- Do the current IT personnel have the skillset to manage the implementation and daily interaction with and monitoring of the cloud service model? Will there be changes to the IT department? For example, will new IT resources be needed, will retraining be needed, or will there be a reduction in headcount?
- Does the entity have the appropriate skill set and capacity to deal with secure connections for the volume of data and transactions being processed with the third-party providers?
- What changes will be made to program change controls? For example, will a Web portal be set up to allow programmers to make changes to programs being hosted by the service provider?

Performance Management and SOC 1 Review
- Is there a SAS 70 or SSAE 16 (SOC 1) report with the appropriate scope available? If not, what provisions will be made for the engagement team to otherwise obtain sufficient audit evidence?
- Has management reviewed the SAS 70 (SOC 1) report to determine whether the service being provided is covered by this report?

Adding Value through Timely Involvement of KPMG
Companies are making significant investments to implement cloud services with the expectation it will help them drive efficiency, increase flexibility, and manage the ongoing costs of technology. Early involvement of our audit team can provide our clients with timely feedback on their controls over financial reporting that may serve to avoid late “surprises” and costly delays in going live, or remediation efforts after an implementation occurs.

Providing observations and recommendations during the project lifecycle gives the company an opportunity to address risks and redesign controls earlier when it is less costly and more efficient. This can be achieved through conducting a real-time implementation assessment for a company’s cloud services strategy.
The two main objectives of a timely cloud services implementation assessment are to:

- Assess project risks and systems development controls while the project is in process, at a time when evidence is readily available
- Assess client-designed process controls, both automated and manual, at the point that they have been designed, but not necessarily configured and implemented. This allows for observations and recommendations to be provided at a point in time where it is less costly and more efficient for the client to implement any changes.

**Benefits to the Company**

- Real-time feedback to the project team, management, and/or the audit committee with respect to control design and implementation
- Allows management to respond more timely to project and control issues
- Feedback relative to the use of more effective and cost-efficient automated application controls
- Identify risks which could jeopardize project timeliness or objectives
- Provides feedback to management and the audit committee on other matters which may come to our attention.

**Benefits to the Audit**

- In-depth understanding of the impacts to internal control over financial reporting
- Early identification of potential audit and control-related issues and reduces the chances of “surprises”
- Identification of automated controls helping to improve control testing effectiveness and efficiency
- Information over integrity of underlying financial data
- Updated audit documentation relative to changes in IT, new processes, and new controls to help facilitate efficient audit planning, walk-throughs, and control testing

**Assessment Outputs**

- Assessment of the design of automated and related manual controls, providing for anticipated selection of controls by the audit team for efficient and effective ongoing audit testing after the system goes live
- Feedback to project team, management, and the Audit Committee with observations and recommendations identified as a result of assessment activities