KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

May 2017

Risk and Performance Quarterly

Cloud Computing: Critical Risks Small and Mid-Sized Organizations Should Address

By Larry Baye, Principal and Mark Bednarz, Partner

For most small and mid-sized organizations, cloud computing is now a widely-accepted, convenient transformative technology solution that relies on a service provider to deliver a shared pool of computing capabilities (e.g. servers, storage, routers) to its customers over a private, public or hybrid network.

Whether the user access is via laptop, desktop, mobile phone or some other personal device, the virtualized computing resources are made available for use on an on-demand basis that can be scaled upward or downward to meet a wide array of customer requirements. From a customer's standpoint, you provision and pay for what you consume and, typically, require less technical support staff, while the provider invests in acquiring, deploying and managing the computing resources.

Provider Services

Typically, the provider offers one or more of the following services:

- **Software-as-a-Service ("SaaS")** like Microsoft 365, Dropbox or Google Docs that allows the customer to use the vendor's application software through a web browser. For example, a town or village may use a hosted system that supports tax appraisals and collections, purchasing and payables, accounts receivable, fixed assets, budgeting, maintenance, financial reporting and analysis, and, in some cases, their school districts as well.

- **Platform-as-a-Service ("PaaS")** such as Google App Engine or Force.com that permits the customer to run either its own software or licensed applications on the platform provided by the vendor. For instance, a consumer products company that is building a proprietary marketing system that incorporates multi-channel data from such sources as retail outlet point-of-sale, mail orders and department stores which will allow them to better forecast sales and know how the assortment of items that should be manufactured based on demand by channel. By using a PaaS model, the customer can model performance, storage and other computing requirements before they migrate the application to their own internal environment.

- **Infrastructure-as-a-Service ("IaaS")** like Rackspace that provides the customer with processing, storage, network and other capabilities on the vendor's resources that can be quickly made available as needed. A business that is launching what they expected to be a hot new service during the Thanksgiving to Christmas holiday season but had no idea as to the level of web-based demand derived benefit by relying on a third party equipped to handle what proved to be large system load variations.

Cloud Computing: Then and Now

While cloud computing may appear to be a new concept, its genesis traces back to the concept of service bureaus and application service providers, where vendors hosted centralized business applications on behalf of customers and processed their financial transactions. Interest in and usage of cloud computing can be anticipated to continue to rise, especially in organizations looking to offload the maintenance of their systems, provide remote access to their systems if a disaster impacts the location where their internal servers reside and/or tackle resource-intensive “Big Data” projects.

Risks and Hotspots

With every new technology that emerges on the horizon, there are always new risks that have to be addressed to ensure that the organization is properly protected. Cloud computing is just the latest example. The time for identifying concerns and resolving them is during the solution evaluation (“due diligence”) stage and while negotiating a service agreement, not when you are already operational. However, there may be a second window of opportunity when the contract is subject to renewal. Here are some of the hotspots to focus on:

- **Cloud Computing Provider Viability** — In doing business with any information technology vendor, gaining insight into their service offerings, business profile and financial health is essential if you expect the relationship to endure over time and you end up relying on their services and support. Industry analysts continue to forecast that pricing and profitability pressures will force consolidation among the providers so focusing on their “staying power” is important. At a minimum, an agreement should have an out clause to avoid perpetual vendor lock-in, including the right to evaluate options with proper notice in the event of an ownership change.

- **Service Level Commitments** — The vendor should be prepared to commit to a set of metrics that define their performance. The metrics may focus on response time, latency, throughput, lead time to provision more/less computing resources, help desk availability and support, tiered service levels and other meaningful indicators of service and support. Identifying metrics that the customer views as relevant to their success are far more relevant than statistics that are simply indicators geared to optimizing the technical performance of computing resources. Remedies in the event of poor performance should be part of the negotiation process.

- **Sensitive Information Should Be Secured** — Information pertaining to personal data that is classified as personally identifiable information (“PII”), such as social security numbers; protected health information (“PHI”) under Heath Insurance Portability and Accountability Act (HIPAA), like patient medical data; financial data, such as credit cards; and, a business intellectual property, like customer and pricing lists, product design specifications are assets that are generally considered to be sensitive and protected by law and regulations. Such data could be made available to authorized users on a confidential basis, but with the expectation that the vendor embraces leading industry practices for protecting the data and maintaining its integrity, whether in use, in storage or during transfer.

One apparel company discovered that while they were designing a new fashion line, its style specifications residing in a cloud environment were “leaked” and used by a competitor to quickly produce “knock-off” low cost and quality versions of the same clothing item; only a discerning eye could see a difference in stitch count if they compared both garments or that the lower priced item would fade during washing.

Under a cloud computing model, understanding the applicable regulations, the types of applications in use, what data protection safeguards (e.g. access policies in place, segregation of one organization’s data from another, use of encryption) and how the vendor would respond to a breach/incident are just some of the elements that must be addressed upfront.

- **Ownership, Usage, Transfer and Storage of Information** — Most customers assume that the data residing on the provider's systems and system usage profiles are proprietary in nature. However, there have been instances where vendors have taken liberties with such information because it has value, including in aggregated form. Policies, procedures and controls must be in place to ensure such practices do not occur and the contract should reinforce these requirements.

- **Audit Rights Provisions and Service Organization Report ("SOC")** — Reputable providers should make available for customer review a SOC report that sheds light on the processes and controls in place at the service organization. The SOC 1 report type focuses on financial processing and controls while SOC 2 pertains to security, availability, processing integrity, confidentiality and privacy. Be sensitive to situations where the SOC 1/SSAE 16 carves out certain functions, including those that may be handled by other parties and not covered by the controls testing described in the report. Customers should try to preserve the right to conduct their own audit of the specific services and systems to ensure that the practices described in these reports apply to their data.

When PKF O'Connor Davies has been engaged by clients to perform such audits, some of the issues we have uncovered concern billing errors, infrequent or superficial security risk assessments that would help identify emerging vulnerabilities and threats, questions regarding the performance, functionality and maturity of the underlying technologies as well as the depth of the cloud computing provider's support staff.

- **Termination Obligations** — Mapping out a course of action for the eventual termination of the vendor relationship is an element of the contract that a customer must address upfront. Some vendors impose exit fees; others require early notice. At a minimum, the organization will likely need assistance in migrating their data to the replacement environment (whether another vendor or internal system) and may require access post-termination to technical support expertise. It is essential that the customer receive positive confirmation that the vendor purged their data and specifics as to how this task was accomplished and verified. Customers have been named in lawsuits years after termination because a former provider's systems were breached and the deleted data was accessible to the hackers from backup files. Further, if a vendor fails, customer data should not be "held hostage" while the bankruptcy plays out in court.

- **Disaster Recovery/Business Continuity Arrangements** — In the event that some disaster caused an extended computing outage at the provider's facilities, understanding their Disaster Recovery and Business Continuity provisions are critical unless the customer determines that the services provided are non-essential or has standby procedures to sustain their operations. A reliable provider would be expected to be able to communicate to the customer their strategy regarding scheduled backups, insurance coverage, redundant systems that are synched, what lead time is necessary to effect a switch over, what load level or performance constraints might exist, whether the primary and alternate datacenters are situated in the same geography and might be exposed to the same event, broadband availability options, etc.

Be Proactive

The benefits of cloud computer services are enormous, but so are the risks. Knowing these risks and finding out the answers to the subjects we raise here will serve you well – whether you are just getting involved with cloud computing, renewing your contract or managing the service.

Contact Us

If you have questions regarding these technologies, how these models might benefit your organization and what changes should be made to your risk and control posture to accommodate cloud computing, feel free to contact the Risk Advisory Group at PKF O’Connor Davies, LLP. Reach out to Larry Baye, Principal, CMC, CISA at lbaye@pkfod.com or Mark Bednarz, Partner, MS, CPA, CISA at mbednarz@pkfod.com.

About PKF O'Connor Davies

PKF O’Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O’Connor Davies is ranked 28th on *Accounting Today’*s 2017 “Top 100 Firms” list and is recognized as one of the “Top 10 Fastest-Growing Firms.” PKF O’Connor Davies is also recognized as a “Leader in Audit and Accounting” and is ranked among the “Top Firms in the Mid-Atlantic,” by *Accounting Today.* In 2017, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O’Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in 440 locations, in 150 countries around the world.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.