# CLOUD COMPUTING: IS YOUR COMPANY WEIGHING *BOTH* BENEFITS & RISKS?

**Toby Merrill**

ACE insured.™

# CLOUD COMPUTING: IS YOUR COMPANY WEIGHING *BOTH* BENEFITS & RISKS?

**Toby Merrill**

**April 2014**

**Cloud computing is a landscape-altering technology that is enjoying increasing rates of adoption — often implemented, however, without taking sufficient risk management precautions. Risk managers need to have a deep understanding of what cloud computing is, and why they need to be aware of it. While there are numerous advantages to adopting the cloud, there are also abundant risks, and having a comprehensive risk management plan in place is critical.**

## Part I: What Is Cloud Computing, and Why Should Risk Managers Care?

Cloud computing has become, among other things, a buzzword nearly everyone has heard, but very few truly understand. And still fewer observers of this technology grasp all its implications for the future — largely because those effects are not yet completely clear. This, in turn, might be because cloud computing is closer to the infancy of its development: so many of its benefits and risks have still to be fully realized or understood. What *is* clear, however, is that the cloud is poised to do nothing less than redefine and take over the Information Technology (IT) landscape and, with it, the way companies around the world do business.

But what exactly *is* cloud computing, and how does it impact the work of risk managers?

Rather than jump into overly technical definitions of the cloud, we'll begin with a broader description of its potential for transformational impact, particularly as a new utility.

Cloud computing has the potential to not only become the defining technology of the twenty-first century, but also the defining utility, just as electricity was for the twentieth. As Nicholas Carr, author of *The Big Switch: Rewiring the World from Edison to Google*, observes, "What happened to the generation of power a century ago is now happening to the processing of information. Private computer systems, built and operated by individual companies, are being supplanted by services provided over a common grid — the Internet — by centralized data-processing plants. Computing is turning into a utility, and once again the economic equations that determine the way we work and live are being rewritten."

It is important for risk managers to recognize that, in the not-too-distant future, a majority of companies, both large and small, will utilize the cloud for some aspect of their business. In fact, according to ACE policyholder data, 59 percent of ACE's Professional Risk policyholders are *already* utilizing the cloud in some way.

As we've mentioned, the cloud has many differing definitions. In fact, there is a multitude of terminology both surrounding and describing variations of the cloud.[1] But, as our focus here is on risk management, we'll concentrate on key definitions that will help risk management professionals get a handle on its benefits and potential risks.

Cloud computing refers to a menu of hosting services usually provided over the Internet on a usage or metered basis, while at the same time leveraging infrastructure shared by multiple customers. Put more simply, cloud computing involves the sale of computer software and hardware "as a service," which means that an organization no longer needs to purchase either; it can instead rent them via the cloud.

Meanwhile, the cloud itself is operated and maintained by cloud service providers (cloud providers) through networked "server farms," which offer their subscribers unlimited availability and data storage, along with seamless access to software, applications provisioning, and automatic upgrades.

To take a closer look at what this actually means, we'll refer back to our electric utility comparison. When we use any appliance that requires electricity, we know that the power will not only be there, it will be sufficient to run our appliance. What we don't know is where, and from what source, the electricity comes from — whether it was from a nearby nuclear power plant, a hydroelectric facility, or a wind farm. Cloud technology is similar. We know it will be there and be sufficient, but we don't know what kind of hardware our data is stored on, nor do we always know where it is stored. The cloud is basically a computing power plant, while cloud providers like Amazon, Microsoft, Rackspace, and Verizon Terremark are computing power companies.

Diving a little deeper, there are some basic definitions that risk managers need to know in order to manage the risks presented by the cloud. First, there are various deployment and delivery models that an organization can select from the cloud.
(See sidebar on page 2, *What is the Cloud?*)

Each deployment and delivery model transfers more — or less — control from the organization to their cloud provider. Two of the most common deployment models are the private and the public cloud. A *private* cloud is the most secure model, and it consists of a series of *dedicated* networks, thus offering the highest degree of *control* to the organization. This model is similar to the traditional computing model; it provides many benefits, but at greater *cost* to the organization. A *public* cloud, by contrast, consists of a series of networks that are *shared* among a number of organizations, thus transferring more control to the cloud provider while offering greater *savings* to the cloud subscriber. According to ACE's Professional Risk policyholder data, among policyholders utilizing the cloud, the split between private and public is fairly even, with 44 percent of policyholders utilizing private cloud deployment and 42 percent utilizing public cloud deployment.[2]

In a similar vein, various delivery models are also available in the cloud. The most basic delivery model is known as Infrastructure as a Service (IaaS). Providers of IaaS include Amazon, Google, Microsoft, AT&T, and Verizon Terremark, among many others. With this delivery model, the organization maintains control over the data stored on the cloud, as well as access rights and data protection.

Another prevalent delivery model is Software as a Service (SaaS), where providers offer a hosted software solution and manage all aspects of the applications on behalf of their customers. Providers of common consumer products that run as SaaS include Netflix, Dropbox, Gmail, Spotify, Facebook, LinkedIn, Instagram, and Twitter; some providers of common business products that run as SaaS are Google Docs, Microsoft Office 365 and Salesforce CRM. With this delivery model, the entire application and service resides on the cloud, and that transfers much overall control to the organization's cloud provider.

## What is the cloud?

Cloud services are divided into four deployment models and three main service categories.

### Deployment Models

**Public Cloud:** Data is stored on shared servers, and is not separated from the general population. Facebook and Gmail are examples of services where data is stored on a public cloud. This is a more cost effective solution.

**Private Cloud:** Data is stored on dedicated resources — not shared servers. This is less cost effective, but often the choice when sensitive information is present.

**Hybrid Cloud:** Data is stored on a combination of dedicated and shared resources.

**Community Cloud:** Data is stored on shared servers, but customers are grouped together by some level of organization. This type of service is often implemented when cloud providers need to manage compliance obligations, such as HIPAA.

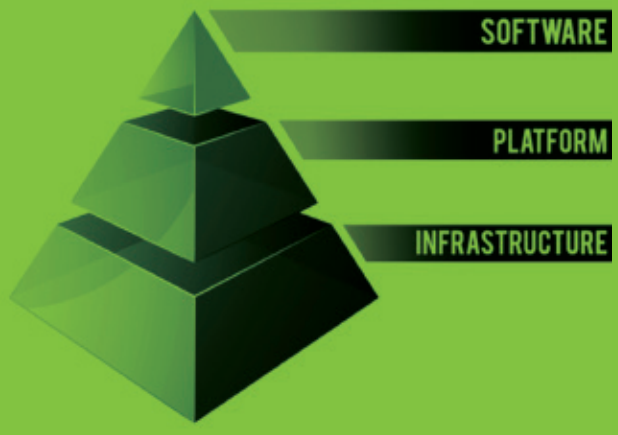
### Service Categories

**Infrastructure as a Service (IaaS):** IaaS providers are the owners of the physical location of their cloud storage. This includes providers such as Amazon, CSC, Microsoft, Rackspace, and Verizon Terremark. IaaS providers provide the physical security, power, compute, storage and networking resources.

**Platform as a Service (PaaS):** PaaS providers are common to the software development environment. They provide not only the infrastructure, but also the development environment to create applications and, in some cases, host them as well. Force.com and Microsoft Azure are two examples of PaaS providers.

**Software as a Service (SaaS):** SaaS providers manage almost all aspects of the infrastructure, platform, and software. SaaS enables the customer to use the software application, without developing or maintaining the installation or platform itself. Customers require only minimal in-house configuration and support resources. Examples of SaaS providers include Salesforce.com, Office 365, Google Apps and Yahoo Mail.

*The pyramid below depicts the Cloud Stack, which is how many technologists refer to the relationship between the three service models.*[17]




*Understanding the Cloud Computing Stack, © Diversity Limited, 2011.*

So what does all this mean for risk managers? To begin with, in the same way that organizations no longer generate their own electricity, as nineteenth century millworks used to do, and instead access it from third party providers, the organizations will no longer own parts of the software and hardware they need to run their many business functions. Depending on the services they outsource to the cloud, organizations will rely on cloud providers to offer the latest version of their software applications, store their sensitive data, back up their servers, and make that cloud-stored information available on their — and their employees'— devices, 24 hours a day, 7 days a week.
(See sidebar on page 4, *BYOD: Bring Your Own Device*)

This change brings with it a large increase in the potential risk that every company faces when operating its business through the cloud. It will be critical for risk managers to closely monitor existing risks and to anticipate risks that will evolve from an organization's increasing ability to store, analyze, and access its data.

## Part II: How Can Cloud Computing Benefit Business?

In Part I, we offered an overview of the revolutionary changes made possible by cloud computing. In this part, we'll discuss the potential benefits of this new form of computing and what it offers as a service useful for business. While there is an extensive list of benefits made available by cloud computing, we will focus our attention on the most impactful ones, such as reduced technology cost, speed and scalability, and enhanced security and backup capacity.

### Top Five Benefits of Cloud Computing

#### Reduced Infrastructure Costs

Computing power is provided to cloud subscribers for a fraction of what it would cost to produce on their own. And, like the electric grid, few companies can afford the computing capacity that a cloud provider, practicing economies of scale, can offer. So the cloud eliminates the need to invest in standalone servers and software that are capital intensive but not in use a majority of the time. The cloud can also help eliminate or reduce such overhead costs as management, IT personnel, data storage, real estate, bandwidth and power. It is important to note that cost saving can vary depending on the deployment and delivery model selected. For example, infrastructure savings are generally greater when leveraging *public* cloud implementations as opposed to *private* cloud implementations. Another cost savings occurs in the area of upgrades. As computing resources become obsolete they must be replaced, in order to ensure operational efficiency. Additional cost savings occur through cloud providers absorbing the expenses associated with software upgrades, hardware upgrades and the replacement of obsolete network and security devices. Maintaining a computing infrastructure requires repetitive capital investment, as the cycle of obsolescence repeats itself, and does so — essentially — forever. The cloud can reduce the costs associated with obsolescence by transferring some of those costs to the cloud provider.

It is important for risk managers to recognize that, in the not-too-distant future, a majority of companies, both large and small, will utilize the cloud for some aspect of their business.

#### Capacity, Scalability and Speed

Three additional key benefits of the cloud lie in its ability to deploy capacity, scalability, and speed. A cloud subscriber no longer has to purchase more computing capacity than is needed at any given time, since the cloud is exponentially scalable. One example of this can be found in the retail industry. At the start of the holiday season in 2013, online traffic for retailers increased 200 percent in desktop use and 400 percent in mobile use.[3] Maintaining this level of computing capacity year-long is both expensive and wasteful. In fact, the excess capacity that Amazon experienced once it had developed its own cloud network was a large reason they became a cloud provider themselves.[4] Cloud computing enables businesses to ramp up their capacity during peak times, then ramp back down to appropriate levels during the year.

Like the utility of electricity, the cloud can stretch or shrink according to the varying needs of individual subscribers. And, by leveraging the cloud, enterprises no longer have to invest time in the purchase and set-up of hardware, software and other resources required for an expansion of existing services, or the development of new services. With the availability of on-demand cloud resources, new configurations can be up and running within hours.

This is particularly valuable because innovation, regardless of the size of the enterprise, springs from constant experimentation and the ability to try out new ideas. Cloud resources provide the means to innovate without extreme investments in computing technology. They also provide the freedom to expand existing services, without the fear of either wasting resources with overcapacity or having insufficient capacity to meet business requirements.

**Security and Backup**

Public cloud computing is built on a backbone of data security, in combination with geographic redundancy for maximum availability. To ensure both, cloud providers invest heavily in physical as well as data security. Most enterprises would be hard pressed to reproduce the physical, organizational, and technical security teams employed by major cloud providers. And most enterprises would not be able to install security teams at multiple locations in order to provide redundancy. In fact, many enterprises' first foray into cloud computing was to leverage cloud storage through data replication or encrypted backup solutions. Because of the numerous data centers and high availability technology that cloud providers maintain, they are able to provide these services far better than a single enterprise.

**Availability, Geography and Mobility**

A major driver of cloud usage is its ubiquitous availability. Cloud technology offers access, via the Internet, to anything stored in the cloud at any time and from any location — in other words, anything, at anytime, anywhere. Consumer applications like Dropbox and iCloud are good examples of how useful and popular always-on and always-available applications have become. Customer Relationship Management (CRM) software applications like Salesforce and Microsoft CRM further illustrate how leveraging the cloud — in this case through mobile technology — can greatly benefit organizations. SaaS applications like these have become vital to sales representatives, and in a relatively short time.

**Regulatory Compliance**

Another major enterprise benefit of the public cloud is the fact that many of the security requirements of regulatory compliance frameworks are normal attributes for cloud providers. For instance, data backups, along with power redundancy, system testing, network monitoring and penetration testing are all standard operations for cloud providers. And many cloud providers have offerings that assist customers in meeting regulatory or industry requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA).

**BYOD: Bring Your Own Device to Work?**

Bring Your Own Device, or BYOD, refers to the cost-effective and employee-friendly policies some companies have adopted, allowing employees to bring their own smartphones, tablets, and laptops to work, then use them to access privileged company information and applications. There are good reasons why a company would permit this. Electronic devices personally owned by employees are often newer and more advanced than the equipment deployed by IT departments. And companies can save money by no longer having to buy and license second or third devices for their employees (for example, smartphones in addition to desktop computers, or smartphones and laptops in addition to desktops).

Of course, companies should consider the risk implications of allowing access to corporate data via employees' personal devices — devices over which the company exercises little or no control. Here are five specific risks that should be addressed prior to rolling out a BYOD policy.[18]

**Unknown Third-Party Access via Mobile Apps:** When employees download mobile apps for their personal use, they also allow unregulated third-party access to any corporate information stored on their devices. These mobile apps may be pre-infected with malware that can exfiltrate sensitive company information from their devices.

**Lack of Monitoring:** Companies will want to have as much control over BYOD devices as possible — including capturing data leakage and usage. This results in a constant tension between employee privacy and the company's risk-containment measures — logging and monitoring data in use and data in transit.

**Device Management:** This employee-company tension is especially clear with regard to device management policies. These policies might range from limiting which devices are supported, to determining whether or not BYOD devices will be subject to a device management program, to requiring passwords and additional security are needed. Companies may also determine the need to use "remote wipe" capabilities, where a single incorrect login could mean that all of an employee's personal data — not just company data — is instantly erased.

**Data Management and Compliance:** Companies subject to compliance obligations may find it not only difficult to convince auditors that their data is adequately protected, but also difficult to provide validation with evidence. As a result, information security teams will need a documented list of data management policies, along with a list of third parties and their data-storing devices.

**Merging Personal and Company Time:** Employees relying on their own devices at work tend to access their personal email and applications more readily, thus increasing the likelihood of engaging in personal activities on company time.

### Hidden Benefits

In a competitive global economy, the market advantage goes to organizations with strong technical leadership — those that are leveraging the latest technology resources. But there are two additional cloud benefits that most overlook. The first is that, when an enterprise migrates its resources to the cloud, this frees their IT executives' time to focus on growing the business by thinking and acting strategically, instead of being saddled with the day-to-day oversight of in-house technology maintenance.[5] The second benefit is that, while migrating data systems is one of the most challenging aspects of a corporate merger, cloud-based systems make that migration much easier and less time-consuming.

## Part III: What Are the Risks of Cloud Computing?

We've looked at the groundbreaking changes that cloud computing makes possible, along with the substantial benefits it offers business, so now we'll turn to the risks of this new technology. By way of illustration, smartphones that allow us to access email, send text messages, access Facebook and surf the Internet — all cloud computing functions — have become virtual extensions of ourselves. In our personal and work lives, they let us perform in seconds a whole range of tasks that used to require far more time and physical effort. But when a smartphone is lost or stolen, we lose not just a telephone, but also an essential key to every area of our lives — our portal to the world that is available to us online.

That said, accessing Amazon with your smartphone wouldn't — if there were an interruption of service — yield the same consequences for *you* that it would for a *company* relying on the cloud to access its data and keep it safe. For you, it would be an annoyance and an inconvenience. For a company, a cloud outage or data breach would be a disaster; the cost to business could be considerable. As a result, being aware of all the potential risks, and practicing due diligence when hiring cloud providers, are steps that are more than recommended — they are essential.

## Top Five Risks of Working with Cloud Service Providers

### Contracts

One of the most significant yet frequently overlooked risks of cloud computing lies in the cloud-biased contracts offered by cloud providers. Risk managers have historically worked with their legal departments to negotiate service provider contract terms to be less "vendor-friendly" and to mitigate any losses caused by service providers by holding the providers financially responsible. But cloud providers haven't been willing to offer the usual indemnification, limitations of liability or other terms — particularly pertaining to privacy and data security. There are a number of reasons cloud providers cite, but the most prevalent are that these additional duties and obligations threaten the lower price model for cloud computing and, since cloud providers don't know what their data subscribers are storing on the cloud, they can't be held liable for segregating and securing subscriber data.

Regardless of the reason, many cloud providers are not only unwilling to take the financial risk contractually, they transfer that risk back to their subscribers.

Unfavorable terms in cloud agreements may increase the risk for customers. Key definitions — including, for example, the definition of "security incident" — may not be broad enough to trigger appropriate incident response obligations and address a customer's regulatory requirements. Most cloud providers will also push back when customers attempt to contractually require specific security measures, or even more general "reasonable security" standards. Customers may also want to contractually limit the subcontractors (and "sub-cloud" providers) that a cloud vendor utilizes to store or process the customer's data. Without these limitations, a customer may find that its data is two or three steps removed from the primary cloud vendor.

The failure to negotiate robust incident response and security and forensic assessment rights can also pose risk. In this context, cloud providers should be viewed as an extension of the customer's IT environment, and customers should attempt to obtain as much control as possible contractually. If a cloud provider suffers a breach that impacts the customer's information, but that provider does not have a contractual duty to provide notice of the breach, remediate and cooperate, then the customer may not be able to reduce its legal risk and comply with regulatory obligations.

Finally, without significant bargaining power or competitive leverage, it is very difficult to get cloud providers to agree to indemnification and unlimited liability for privacy and data breaches. Cloud provider contracts typically start with a limitation of liability (both a monetary limit and consequential damages disclaimer) that is often inadequate to cover a customer's potential losses in the wake of the cloud provider's data breach. Without adequate contractual recourse, customers can find themselves being hit with the full liability of a data breach that technically was not their fault.

> Being aware of all the potential risks, and practicing due diligence when hiring cloud providers, are steps that are more than recommended — they are essential.

**Loss of Control**

Another significant risk that cloud computing presents is a general loss of control over data transferred to the cloud and network availability outsourced to the cloud. For instance, in a more traditional IT setting, organizations have the ability to assess and adjust their systems so they are compliant with applicable regulations and standards. For instance, an organization sending data to a cloud provider located in a member country of the European Union (EU) must follow the requirements of the EU Data Protection Directive (95/46/EC).[6] But an organization can be deemed noncompliant if their data was transferred to a jurisdiction that violates that rule. And since many cloud providers use data warehouses located in multiple jurisdictions, compliance represents an increased risk. Further, the ever-changing regulatory landscape itself increases the risk of violation.[7] Recent events at the National Security Agency (NSA), and concerns abroad about U.S. technology companies housing non-U.S. resident data, have only amplified that potential risk.[8]

Another control risk amplified in the cloud is data *forensics*. Should a breach occur on a system, it is important to forensically determine what data may have been compromised, but the cloud presents a number of challenges for that effort. First, the cloud provider may limit access, or simply not allow your forensic examiners into the cloud environment. Second, in a public cloud, your data may be intermingled with data from other companies, making it difficult to do a simple investigation. Third, this could result in additional legal challenges in accessing the data — as your data may be shared with an organization (or organizations) that restrict third party access. A key to limiting legal and operational risk associated with cloud provider data breaches is the customer's ability to independently conduct a forensic investigation of the incident, which typically includes taking an image of potentially compromised computers.

Additional loss of control concerns within the cloud can include:

- In a cloud environment, you don't get to choose your neighbors — a factor that can impact both your risk and your productivity. For example, if your data is stored in the same infrastructure as a retailer, you can experience the same issues they do during the holiday season — even if it has nothing to do with your core business.[9]
- As outages by cloud providers are becoming more common, an organization relying upon a cloud provider to access the critical data that operates its network may lose considerable control should their cloud provider experience an outage.
- Many SaaS cloud providers lack the technology to operate their cloud environment; instead, they outsource their infrastructure to a third party IaaS cloud provider. This provider-of-the-provider arrangement can make it difficult to keep track of regulatory compliance requirements, data incident reporting, contractual liability — and the list goes on.

**Aggregation Risk**

A frequently highlighted benefit of cloud computing is the increased security level it provides, and for most companies, this is a valid benefit. However, just as most companies choose to deposit their money in large banks because of the security they offer, doing so also increases the risk of more sophisticated criminal attacks, since the aggregated wealth of a large bank is far greater than the individual wealth of a single company. Criminals have access to highly skilled professionals, funding and the patience to organize well-devised attacks. George Clooney and Brad Pitt depict this type of collaboration well in the movie *Ocean's Eleven,* where they join together to take down three casinos. The world of cyber-crime is no different, as advanced attacks — often referred to as Advanced Persistent Threat (APT) attacks — against large, highly-sophisticated technology companies and other institutions continue to increase. The cloud creates a new aggregation exposure that organizations have never faced before. At the same time, aggregation risk is another reason why cloud providers are reluctant to offer more favorable contracts to their subscribers.

**Cost**

The most common benefit that organizations highlight for their adoption of cloud computing is the reduction in technology costs — and no one can dispute the up-front savings the cloud offers organizations. Potentially, though, there are a number of hidden costs with cloud computing that many may not have considered. For example, what are the costs associated with transferring your data and network to another cloud provider? Once a company's data resides on the cloud it becomes increasingly reliant on its provider; cloud providers know this and could easily make moving to another provider difficult.

Another benefit of the cloud that actually contains a hidden cost lies in the area of regulatory compliance. While many cloud providers deservedly tout their compliance with certain standards as a key benefit and a potential costs savings, there is the easily overlooked responsibility and related cost of conducting vendor due diligence — since most regulations and standards hold the organization responsible for their vendor's malfeasance or non-compliance. So while you may outsource your data or network to a third party, you can never outsource your risk or liability.

Many organizations have also found that subscribing to one cloud is not enough. And here's why: services provided through a cloud provider involve connections over the Internet, which is subjected to periodic congestion and outages. Cloud services can also be degraded by malicious attacks on it or on an upstream supplier. One way for organizations to lessen these risks is through the service redundancy provided by contracting with multiple cloud providers.[10]

Finally, each risk identified earlier under "Loss of Control" — most notably data forensics — can also contribute to an increased cost for the cloud. Other costs that need to be considered include further legal expenditures and tax implications, as well as audit and oversight.

**Data Security**

Data security is a key benefit that many cloud providers rightly cite as part of their marketing efforts, since data security can benefit many companies not able to invest significant resources in securing their own data and systems. However, as just mentioned, outsourcing all your data to a single provider also creates aggregation risk. And, what many organizations unfortunately fail to recognize is, it's *their* responsibility to secure their data before sending it to the cloud, as cloud providers generally will not guarantee the security of data stored in their cloud. In fact — as also mentioned earlier, under "Contracts" — most cloud providers will limit their contractual exposure entirely. Equally important is the fact that most statutes and regulations hold the data owner (typically the organization with a direct relationship with an individual's personal information) responsible for any breach or mismanagement of that data. (See sidebar opposite, *Big Data & Big Data Analytics*).

Finally, as the use of Big Data and data analytics continues to grow, so does the value of the personal information that organizations store in the cloud. At the same time, the definition of what constitutes personal information — or other unique identifiers — also continues to expand. This is important for organizations that are storing Personally Identifiable Information (PII) on the cloud to note now, because what might not be considered PII today may be five or ten years from now. For example, earlier this year, California expanded the definition of personal information in its breach notification statute to include "a user name or email address, in combination with a password or security question and answer that would permit access to an online account."[11] As a result, when that data isn't properly secured today, it could expose the organization when new statutes or regulations require the protection of such things as zip codes, device IDs and so forth. But it's important to keep in mind that it is the combination of all these elements that could potentially result in greater risk.

## Part IV: Making Cloud Computing Work for Your Company — Balancing the Benefits and Risks of the Cloud

When organizations decide to migrate data to the cloud, they usually focus on the dazzling benefits. Value can be realized through reduced costs, the ability to access data from anywhere, being able to redirect IT staff away from daily nuts and bolts tasks to mission-critical initiatives, and much more. Alas, every cloud benefit has an accompanying cloud risk. Too often, organizations overlook or ignore those risks by failing to consult risk management professionals before moving ahead.

### Big Data & Big Data Analytics

Big Data refers to data sets that are too large for typical business database software tools to capture, store, manage, and analyze. Cloud providers offer cost-effective, scalable solutions for enterprises interested in developing Big Data analytics programs to provide improved customer service, better business opportunities, or detect fraud. Even large banks and healthcare systems find that developing such programs is impossible in-house — both because of infrastructure limitations, and because limited budgets can't meet the resource costs needed up front for Big Data analytics. So the cloud plays a significant role in the development, deployment, and optimization of Big Data applications.

Here are a few examples of Big Data in action[19]:

- Insurer United Healthcare leverages Big Data to detect potential cases of medical fraud and identity theft. It does so by looking at speech-to-text call center data to mine potential attrition candidates (those who don't sound like happy clients) and propose remedies.
- Intermountain Healthcare, a Utah-based system of 22 hospitals, 185 health groups, and an affiliated insurer, leverages Big Data analytics with outcomes analyses of more than 90 million electronic health records. They study the relationship between treatments and outcomes, hoping to improve existing medications and develop new ones.
- Morgan Stanley leverages Hadoop to implement the Big Data analytics they use to analyze customer financial goals and provide better investment opportunities, while also providing improved web and database log analysis for their IT division.

An organization about to send its precious data to the cloud needs to use the same level of due diligence that it would when constructing a building in an earthquake zone. That analogy is apt because there are many risks and control issues that need consideration if an organization wishes to mitigate as many pitfalls as possible.

We don't have room to discuss all of them here, but we'll look at the core areas deserving of careful consideration by any enterprise contemplating a cloud migration: privacy by design and culture; shared security and related responsibilities; control and liability; and due diligence and vendor management programs.

**Privacy by Design and Culture**

Privacy has become an essential human right protected by laws, statutes and regulations throughout the world. Migration into the cloud environment should be an extension of "privacy by design" principles[12] already in use — since organizations should incorporate privacy requirements during their development of new systems, products, and services. Many, in fact, are asking their Chief Privacy Officer (CPO) or Chief Information Security Officer (CISO) to perform a *Privacy Impact Assessment*[13] — a process which helps identify and reduce the privacy risks of products and services under development.

In the same vein, organizations should choose the data and applications that, when migrated to the cloud, will increase their efficiency and connectivity. But while making those choices, they should use data classification to identify, organize and secure all sensitive data — prior to actually migrating data and applications into the cloud. It may also be prudent to start with data and applications that pose a low privacy and data security risk (and are not business critical), before moving to higher privacy risk applications, especially those that touch highly sensitive private information. For example, only 21 percent of ACE's Professional Risk policyholders are storing sensitive records on the cloud and, when they do, the vast majority are encrypting that data. These precautions are all the more important because technology companies tend to capitalize on new capabilities as soon as they are available, and only address privacy and security issues once a regulation demands the installation of controls. This is, obviously, a risk-filled situation.

Implementing privacy by design into the organization does more than benefit the products and services of the organization. It also has as a tremendous influence on the culture of its employees. There is no better tool for managing risk than the people that support the processes and technologies that have been implemented. For example, another segment of cloud services that employees are utilizing are personal cloud storage services such as Google Drive, Dropbox or iCloud. Sometimes referred to as Bring Your Own Cloud (BYOC)[14], these services are often used by employees to store, share and collaborate on documents on the cloud, making it easier for them to work on documents from work and personal devices. An organization that has properly embedded privacy and security by design principles into its culture will have privacy-conscious employees that are far less likely to place sensitive data at risk into such services.

**Shared Security and Related Responsibilities**

Risk managers need to keep in mind the fact that data privacy and security responsibilities begin within their own organization before continuing into the cloud. Vital security controls can be overlooked if the allocation of security responsibilities between the organization and the cloud provider isn't fully understood. Think of the security responsibilities divided between an office space tenant and an office building landlord as analogous to those of an organization and a cloud provider. To allocate responsibilities correctly, risk managers should:

- Understand the type of cloud service being utilized, as security responsibilities will vary, depending upon whether it is SaaS, Platform as a Service (PaaS) or IaaS.
- Ensure that the organization has "mapped" its security capabilities, as well as its current responsibilities. For example, healthcare organizations will need to map HIPAA requirements, while all organizations that process credit card payments will need to map their PCI (Payment Card Industry) requirements.

- Outline the security controls available on the cloud platform they intend to use. This is particularly important, as it will be very difficult to assess the risks of moving to the cloud if a cloud provider under consideration isn't fully transparent about their security and privacy capabilities.
- Clearly identify which security responsibilities will transfer to the cloud provider, and which responsibilities will remain with the organization. For example, if your organization has traditionally conducted penetration testing or data encryption, will those responsibilities become your cloud provider's, your continued responsibility or a shared responsibility?

Geographic redundancy is often touted as a strong security benefit by cloud providers, but organizations should assess how cloud providers will deploy this redundancy, and whether it meets the organization's disaster recovery or business continuity needs — while also keeping data compliance in mind. For instance, cloud providers should simultaneously update information throughout their redundancies, but also segregate them to properly to ensure minimal downtime. In the event that one data center becomes adversely affected, this segregation will ensure the backup server location is not impacted as well. Also, geographic redundancy may assist with redundancy but, as noted in Part III, it also increases regulatory risk, as transferring data across borders may violate local privacy requirements. So it is important to fully understand which data centers will be utilized and whether the data being stored in the cloud is subject to any geographic restrictions.

Organizations relying on cloud providers also need to prepare for cloud outages with a backup plan — maintaining their own systems to run business critical applications — just as they use backup generators during electricity power outages. In the end, risk managers should review their backup policies, making sure they are updated to reflect the features and services available through the cloud provider.

Finally, though the cloud can make it easier to comply with regulatory requirements, if your organization is in a heavily regulated industry, like healthcare or financial services, it's wise to conduct a full compliance assessment to ensure that your cloud provider is using proper compliance programs. It's also a good idea to ask an independent third party to confirm your cloud provider's compliance with governing regulations.[15]

Smaller organizations will usually not have the negotiating power to conduct full audits of a cloud provider. However, due to mandatory business associate agreements for the healthcare industry, we are starting to see a small segment of cloud providers that are willing to negotiate vendor agreements, in order to better accommodate cloud subscriber's compliance needs. Risk managers should confirm that the cloud provider they entrust with their critical business applications, sensitive personal and corporate data, and security, is receptive and willing to partner with them in meeting regulatory and compliance challenges. They should also be prepared to make the difficult recommendation of not using the new technology if it sacrifices sound risk management principles.

**Control and Liability**

While companies must sacrifice some element of control in order to utilize the benefits of cloud computing, there are best practices that can help mitigate the security as well as the financial risks associated with this loss of control. First, since organizations have the most control over their data prior to migrating to the cloud, they should assess their potential cloud providers to determine whether they are focused on security, privacy and transparency. For example, risk managers need to know whether the entire cloud platform is being run by the cloud provider directly, or if aspects of the cloud have been outsourced to another "sub-cloud" provider. Not all cloud providers are created equal in providing such transparency, and risk managers should be involved in assessments of cloud providers and determining the scope of services and the types of data that will be transferred to the cloud in order to minimize the impact to network security and privacy related risks. There are a number of standards that have and continue to be developed to assist organizations in assessing the quality of cloud providers.[16]

Risk managers need to keep in mind the fact that data privacy and security responsibilities begin within their own organization before continuing into the cloud.

Second, once the organization has chosen one or more cloud providers, the data assessment, encryption and proper encryption key management will be the best options for controlling data access for most companies. But before determining which data set to encrypt, as noted in Part III, it's important to realize that today's definition of personal information or corporate confidential information may be very different than definitions five or ten years from now — and maybe sooner, depending on the nature of the company's business, industry or regulatory activity. In light of continually changing privacy and data security regulations around the globe, organizations storing online usernames and passwords, historically and going forward, have to reassess their risk in failing to encrypt that information.

Since many cloud providers include some form of encryption as a part of their offering, encryption may prove a cost-effective option for organizations. In fact, according to ACE's Professional Risk policyholder data, 73 percent of policyholders that are

transferring sensitive data to the cloud are encrypting that data. As a best practice, organizations should place their encryption keys in a secure environment, one completely segregated from the cloud — through their own encryption key management program, or a third party.

Organizations should also be vigilant about monitoring traffic and activity in their cloud environment, to maintain proper control of their data. And while it remains a challenge to negotiate contractual terms with cloud providers, many are willing to provide enhanced monitoring and security services that benefit the organization. For instance, some cloud providers are willing to provide logs that indicate activity by the cloud provider and its employees in the organization's cloud environment.

Third, although it continues to be difficult negotiating indemnification and limitation of liability provisions in contracts with cloud providers, organizations are having more success negotiating rights to audit and access the cloud platform or infrastructure, especially in the event of a breach. Cloud providers have generally emphasized the shared security approach, and understand that companies using its infrastructure, platform or services have non-negotiable regulatory obligations. Moreover, in light of increasing regulatory and privacy concerns associated with migration to the cloud, organizations should negotiate separate contracts to satisfy and protect their business needs, as well as their regulatory and privacy needs. This will help both parties focus on important but often unrelated issues present in contracts related to services, and contracts related to compliance. For example, cloud providers often analyze their clients' data, and while it may constitute a relatively small part of the total services offered, service contracts request broad consent not only to store, but also to manipulate and analyze that data. These activities can trigger privacy and data security concerns. Having a separate contract will allow organizations to better define what the cloud provider can and can't do with their data.

Fourth, organizations should have an exit strategy, both to maintain control over their data, and to respond to the potential for unpredictable cost fluctuations. Without a proper and quick exit strategy (a two-year contract duration is just not a good strategy), organizations may be locked into a single proprietary cloud provider, even if that provider no longer meets the organizations business or financial needs.[8] Often, the costs associated with migrating between cloud providers and the "gravity" of the stored data will make it difficult, if not cost-prohibitive, to move to another provider. In devising an exit strategy, organizations should:

- Budget for relocation during the initial migration, to ensure that the organization has the financial capacity to move between cloud providers when necessary.
- Plan both a quick exit strategy and a long-term strategy. In light of infrastructure and application reliance on a cloud provider, it will be a challenge to effectuate a timely transfer to another provider, unless the company has taken proactive steps prior to the initial migration into the provider's cloud.
- Consider consistent monitoring and management procedures, such that the organization can evaluate whether the current provider continues to meet its business needs.
- Diversify between private and public clouds to ensure that the organization will maintain some control over business critical applications and data.
- Be sure to understand how the cloud provider will treat the organization's data upon termination of the contract ("shards" of data could remain with the provider in perpetuity). Organizations should confirm that the retained data cannot be reconstituted, and that it does not pose an ongoing data security risk for the organization.

**Due Diligence and Vendor Management Programs**

In the end, creating a privacy by design culture, having clear shared responsibilities with your cloud provider and establishing the proper control and liability is not sufficient; you also need to implement the proper due diligence and vendor management program. Increasingly, cloud customers are developing formal due diligence processes and vendor management programs to assess and manage the cloud-related risks referenced in this paper. In fact, many regulatory bodies — including financial regulators enforcing the Gramm-Leach-Bliley Act (GLBA) — now scrutinize organizations' vendor management programs to ensure that regulated personal data and other sensitive information is protected and handled properly when in the hands of cloud providers and other vendors. While approaches may vary, most vendor management programs contain common elements, including a preliminary data assessment, a security and privacy risk assessment process and standard contract terms focused on data security and privacy.

Under these programs, in order to assess potential risk, cloud customers complete forms that break down the data elements that will be processed by a cloud provider. The initial data assessment will typically allow the customer's stakeholders (legal, security, privacy and business stakeholders) to understand the relative risk of the transaction and proceed accordingly. For example, if only non-sensitive records are being provided to the cloud provider, as opposed to social security numbers or financial account data, less vendor scrutiny may be appropriate.

Once a baseline risk level is established, many cloud customers engage in a security and privacy due diligence process. Again, it is fairly common for customers to have security assessment questionnaires that they provide to the cloud provider for completion. These questionnaires inquire about internal security controls the customer wants to see in place with the cloud vendor, and typically address regulatory requirement concerns around security and privacy. They also inquire about the cloud vendor's use and disclosure of personal information to determine where personal information will be processed and whether the cloud vendor will be using the information for its own purposes or disclosing to third parties (for example, disclosures to third party advertisers). The responses to these questionnaires further allow customers to refine their risk assessment, and feed into the contracting phase of the cloud transaction.

To reinforce their risk assessment and due diligence process, and as part of their vendor management program, many cloud customers create standard data security and privacy schedules to include in their cloud contracts. The purpose of these schedules is to address regulatory issues, provide a mechanism to hold a cloud vendor to reasonable security standards, establish incident response obligations and transfer risk of loss for data breaches or privacy violations caused by the cloud provider. Again, the overall goal is to attempt to contractually create a seamless relationship with the cloud provider and reduce risk as much as possible. The contracting process for vendor management programs is sometimes further refined to allow customers to have pre-established "fallback" positions for certain terms during negotiations with cloud providers. It is not unusual for both a customer's lawyers and security professionals to be involved in the negotiation of these terms.

Overall, a vendor management program can help organizations understand and manage their risks, and the existence of an established and robust program suggests that the organization has fully considered cloud risks.

## A Brief Conclusion

We are at an exciting moment in the evolution of technology; like all such moments, it offers both benefits and risks. The benefits of the cloud are tremendous and impossible to ignore — to do so could put an organization at a considerable competitive disadvantage. And while there is no doubt that organizations face many challenges in adopting the cloud and its related technology, these can largely be overcome with a rational analysis of both cloud provider services and the changing needs of the organization. So the questions that every risk manager must inevitably answer are these: What is the optimal way to balance all the benefits of cloud computing against all of its potential risks? What are the best and most appropriate risk management tools for mitigating those risks, without losing all that the cloud has to offer?

## About the ACE Technology Series:

This is the second edition in ACE's series of technology white papers, designed to offer risk managers an overview of the many benefits and risks of various breakthrough technologies that have begun to reshape business environments of all sizes.

ACE's first technology paper focused on social media as a source of considerable benefit and equally considerable risk. A copy of *Social Media: The Business Benefits May Be Enormous, But Can the Risks — Reputational, Legal, Operational — Be Mitigated?* is available at http://www.acegroup.com/us/privacyprotection.

This second paper focuses on cloud computing, a landscape-altering technology that is enjoying increasing rates of adoption — often implemented, however, without taking sufficient risk management precautions.

## About the Authors:

**Toby Merrill** is Division Senior Vice President, Global Cyber Risk Practice Leader for ACE Group. Mr. Merrill has nearly 20 years of experience in the insurance arena, specifically in underwriting professional liability, management liability, and cyber risk exposures. He previously held the role of Vice President, National Product Manager for ACE's network security, privacy, and technology Errors & Omissions (E&O) liability products in the U.S., where he was responsible for product development and overseeing underwriting operations for those lines, including for multinational businesses. He has authored a number of articles on privacy, network, and social media risks, and speaks frequently on cyber risk and network security topics. Mr. Merrill can be contacted at Toby.Merrill@acegroup.com.

Editorial assistance for this paper was provided by David Navetta, with Information Law Group. Mr. Navetta can be contacted at dnavetta@infolawgroup.com.

## CONTACT US

**ACE USA**
436 Walnut Street
Philadelphia, PA 19106, United States
www.acegroup.com/us/privacyprotection

ACE Group is one of the world's largest multiline property and casualty insurers. With operations in 54 countries, ACE provides commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. ACE Limited, the parent company of ACE Group, is listed on the New York Stock Exchange (NYSE: ACE) and is a component of the S&P 500 index. Additional information can be found at www.acegroup.com.

The opinions and the positions expressed in this paper are the author's own and not necessarily those of any ACE company. Insurance is provided by ACE American Insurance Company, Philadelphia, PA, or in some jurisdictions, other insurance companies in ACE Group. This publication is for educational purposes only. The suggestions and information are not intended to be professional or legal advice. The advice of a competent attorney or other professionals should be sought prior to applying this information to a particular set of facts.



## Endnotes:

1 NIST Definition of Cloud Computing: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
NIST Cloud Computing Synopsis and Recommendations: http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf
Cloud Security Alliance Web Site: https://cloudsecurityalliance.org/
PCI Security Council's Guidance: https://www.pcisecuritystandards.org/pdfs/pr_130205_Cloud_SIG.pdf
PCI Security Council Guidance on Virtualization: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

2 The remaining 14 percent of ACE's Professional Risk policyholders utilize hybrid cloud deployment.

3 Kuchler, Margaret. Mobile Retail Traffic Represents 35 percent of the Thanksgiving Holiday Traffic. Akamai.com (2013). https://blogs.akamai.com/retail-commerce/

4 Flinders, Karl. Amazon Web Services Reaches Its 8th Birthday. ComputerWeekly.com (2014). http://www.computerweekly.com/news/2240216103/Amazon-web-services-AWS-reaches-its-8th-birthday

5 Davenport, Thomas. The New CIO Is...and Analytical CTO?, Online.WSJ.com (2014). http://blogs.wsj.com/cio/2014/03/12/the-new-cio-is-an-analytical-cto/

6 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995). http://tinyurl.com/6gpkrav

7 Edwards Wildman Palmer LLP. Everyone's Nightmare: Privacy and Data Breach Risks. EdwardsWildman.com (2013). http://www.edwardswildman.com/files/Publication/ce47655d-5868-49d3-9901-e6ef06350e68/Presentation/PublicationAttachment/e8180d9e-76a6-4b86-8153-e873f8f5f9dc/EdwardsWildmanPrivacyWhitePaperMay2013.pdf
Schectman, Joel. Pre-Cloud Encryption Could Prevent Surreptitious Government Data Collection. Online.WSJ.com (2013). http://on.wsj.com/17Ur4GQ
Perez, Evan. NSA Secrecy Prompts a Pushback. Wall Street Journal (2013). http://on.wsj.com/10anhSU
Efrati, Amir. Google Asks for Approval to Report NSA Data Requests. Wall Street Journal (2013). http://on.wsj.com/117zHtv

8 Bracy, Jedidiah. European Parliament Votes in Favor of Proposed Data Protection Reform. PrivacyAssociation.org (2014). https://www.privacyassociation.org/privacy_tracker/post/european_parliament_votes_in_favor_of_proposed_data_protection_reform

9 Wallace, Matthew. The Problem With Noisy Neighbors in the Cloud. AllThingsD.com (2013). http://allthingsd.com/20130225/the-problem-with-noisy-neighbors-in-the-cloud/

10 Mosher, Richard. Cloud Computing Risks. ISSA Journal (2011). http://www.experis.us/Website-File-Pile/Articles/Experis/FIN_Cloud-Computing-Risks_071111.pdf

11 California Civil Code § 1798.82

12 "The concept of privacy by design includes limitations on data collection and retention, as well as reasonable security and data accuracy. By considering and addressing privacy at every stage of product and service development, companies can shift the burden away from consumers who would otherwise have to seek out privacy protective practices and technologies." Protecting Consumer Privacy in an Era of Rapid Change. FTC Report (2012).

13 Department of Homeland Security, Privacy Office. Privacy Impact Assessments. http://www.dhs.gov/privacy-office-privacy-impact-assessments-pia

14 Janssen, Cory. Bring Your Own Cloud (BYOC). Techopedia.com. http://www.techopedia.com/definition/29069/bring-your-own-cloud-byoc

15 The Cloud Security Alliance provides a questionnaire available in spreadsheet format, with a set of questions that a cloud consumer and cloud auditor can pose to a cloud provider." The questionnaire can be found at https://cloudsecurityalliance.org/research/cai/.

16 Various standards that currently exist include NIST, FEDRAMP and Japan's cloud security standards.
Japan's Cloud Security Rules Set to Become Global Standard. Asia.Nikkei.com (2014). http://asia.nikkei.com/Politics-Economy/Economy/Japan-s-cloud-security-rules-set-to-become-global-standard.

17 Kepes, Ben and Rackspace Hosting. Understanding the Cloud Computing Stack: Saas Paas, Iaas. Cloud U, Diversity Limited (2011). http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

18 Phneah, Ellyne. Five Security Risks of Moving Data in BYOD Era. ZDNet.com (2013). http://www.zdnet.com/five-security-risks-of-moving-data-in-byod-era-7000010665/
Baldwin, Caroline. Top Five BYOD Problems and App Solutions. ComputerWeekly.com (2013). http://www.computerweekly.com/blogs/inspect-a-gadget/2013/08/top-five-byod-problems-and-app-solutions.html
Hyman, Jon. Don't Forget These Five Security Issues in Your BYOD Policy. Workforce.com (2012). http://www.workforce.com/blogs/3-the-practical-employer/post/don-t-forget-these-five-security-issues-in-your-byod-policy

19 Eastwood, Brian. Big Data Analytics Use Cases for Healthcare IT. Online.CIO.com (2013). http://www.cio.com/slideshow/detail/126493/Big-Data-Analytics-Use-Cases-for-Healthcare-IT#slide6 //
Bird, Julie. 3 Ways Healthcare Orgs Use Big Data. FierceHealthIT.com (2013). http://www.fiercehealthit.com/story/3-ways-healthcare-orgs-use-big-data/2013-11-01//
Groenfeldt, Tom. Morgan Stanley Takes on Big Data with Hadoop. Forbes (2012). http://www.forbes.com/sites/tomgroenfeldt/2012/05/30/morgan-stanley-takes-on-big-data-with-hadoop/
Manyika, James; Chui, Michael; Brown, Brad; Bughin, Jacques; Dobbs, Richard; Roxburgh, Charles; Byers, Angela Hung. Big Data: The Next Frontier for Innovation, Competition, and Productivity. McKinsey & Company (2011). http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation