Businesses around the world are witnessing a flood of new cloud computing services entering the market. These offerings are making it easier for almost anyone to engage and access, and they cover everything from personal file backup to major production server and application services. Will cloud computing deliver lasting economic benefits to businesses? What is the best use of cloud services and can they be adopted in ways that do not put a business’s risk profile in peril? These are questions that will, and should, be debated in boardrooms for some time to come.

One thing for sure is that the cloud computing trend is putting pressure on traditional IT governance processes to adapt. For businesses to make prudent decisions regarding the adoption of cloud services, IT governance and risk managers need to work closely with business managers to promote understanding of key cloud computing principles and to help establish effective governance practices.

WHAT IS ALL THE FUSS ABOUT?
For those not familiar with the term, “cloud computing” describes Internet-based technology (either software, platform, infrastructure or a combination) that stores and processes information and is provided as an on-demand service.

So what is so new and revolutionary about this? On the surface, it sounds like an Internet version of IT outsourcing. Well, in a way, it is, but with a few important differences. To explain, it helps to use an analogy: Take people who commute to work by driving their own cars, but arrive late due to traffic, roadwork delays and frequent breakdowns (as their cars are old and poorly maintained). Now, they might choose to address this situation by buying navigational devices, upgrading their cars, securing regular maintenance services or even by hiring professional drivers to take them to and from work. This approach would be similar to delivering an outcome using traditional IT service models, with the use of a driver similar to traditional IT outsourcing.

An alternative approach for addressing the situation could be for people to trade in their cars and buy yearly tickets to take the train to work. By doing this, people would essentially be giving up the individualistic approach to commuting and adopting a standardized, technologically agnostic approach to achieving the same outcome. The whole problem with unreliable cars and the costs of driving are replaced with a solution with a completely different cost structure as well as different risks and opportunities. This approach is analogous to transitioning to the use of cloud computing services.

Similar to this analogy, there are several important trade-offs that occur when transitioning to cloud computing from traditional IT (whether in-house or traditional outsourcing). Exactly what these trade-offs are depend on the specifics of the services being engaged, but the typical ones to be aware of are:

• **Flexibility**—When using traditional IT, businesses have almost complete flexibility as to what they do with it because they are in charge of how it is used. With cloud computing, however, flexibility is likely to be more constrained by the way the services are supplied. For example, many Platform as a Service (PaaS) cloud services are kept up to date with current operating system versions, so if a business wants to operate using an older version, it may not be possible or may require negotiation of a more customized (and more costly) service. Some cloud services, such as Amazon’s EC2, offer a lot of flexible options; however, setting them up and maintaining the configurations takes more effort and skill than other out-of-the-box offerings. As a benefit though, a flexible feature of cloud services is the ability to switch them on and off quickly without buying and selling expensive infrastructure and software.
• Security—With traditional IT, businesses are in charge of security—how tightly their systems are locked up, who has access to them, and who else (if anybody) can share their processing and storage capabilities. In the cloud, the service provider controls many of these aspects. They may actually do as good a job or a better job than many businesses, but customers may not have much visibility as to how secure the service is. Cloud customers will also most likely share resources with other businesses without knowing who the other businesses are. For many businesses, this means a major rethink about the way security is governed.

• Reliability and availability—Similar to the analogy, the promise of more reliable and available services is one of the major reasons why businesses are attracted to the cloud. While (arguably) cloud services are potentially more reliable, issues do not completely go away, and there is also less visibility to customers regarding the causes of outages or the issues of reliability. This too requires a different governance approach.

• Scalability—Undoubtedly, this is where cloud computing claims its largest advantage over traditional IT—the ability to readily scale up and down processing and storage requirements without large changes in overhead costs. For many businesses, this capability can lead to major risk reduction, but, again, governance approaches need to adapt to take advantage.

Clearly there are pros and cons of both traditional IT and cloud-based services. But one of the great aspects of the flood of new services coming onto the market is that almost all businesses can benefit—through cost reduction, risk mitigation or both—from the increase in choices available. For this reason, it makes sense to keep an eye on new services as they emerge.

CLOUD ECONOMICS BASICS
To understand the risk and reward profiles of cloud services, it is important to understand the economics behind them. Here is a brief outline of the basics. Essentially, cloud providers are able to deliver services less expensively than in traditional IT service models due to two key factors:

1. Through standardization and abstraction of technologies (e.g., use of virtual machines), they can upscale and downscale storage and processing capability more efficiently. This reduces costs of adding and removing systems as service demands change.

2. Through sharing of IT capabilities across multiple clients with different demand cycles, they can eliminate underutilization of resources. This reduces overhead costs associated with idle capacity.

Figure 1 depicts how these cost savings may look for a business that undergoes periodic peaks and troughs and has high unpredictability in its demand for IT services.

Cost savings derived from:
• Efficiency of upscaling/downscaling as demand changes
• Reduced underutilization from sharing services

Note: Potential savings are greater when more layers of the IT stack are transitioned to the cloud, e.g., greater cost savings for SaaS than for IaaS.
The potential cost differential between the two models is even greater when more layers of the IT stack are transitioned to the cloud. For example, for Software as a Service (SaaS), where software, platform and infrastructure layers are bundled into a single cloud service, cost savings are potentially greater than with Infrastructure as a Service (IaaS), where only hardware layers (e.g., storage, CPU, network) are provided. This is because efficiency increases as more and more components are standardized and bundled together.

As with the transportation analogy, neither approach (traditional IT nor cloud computing) will always be superior to the other. Cloud computing has introduced additional options for IT service delivery. For many businesses, an optimal approach that leverages the best of both models will achieve an improved risk-reward trade-off. Figure 2 depicts how this may occur.

Also, over time, cloud providers are aiming to create even greater cost savings as they capture larger market share and capitalize on economies of scale.

**DECIDING TO DRIVE OR RIDE (OR MAYBE A MIX OF BOTH)**

So if the cost savings from transitioning to the cloud are that compelling, why do businesses not move all their IT to the cloud? This is a fair question that is coming up regularly in boardrooms around the globe. But, unfortunately, the answer is not as simple as it might seem, as there are several other factors to consider, not the least being those relating to risk management, compliance and security.

Therefore, the right answer to the question, “Should I drive or ride?” is: “It depends.” It depends on the nature of the IT service, future growth expectations, the business’s risk appetite, legal and regulatory compliance requirements, and cost. With all these factors to consider, it is essential that businesses carefully think through their IT service delivery strategy and prepare a business case that covers all of these factors. Figure 3 illustrates an approach to measuring risk-mitigation costs so that they can be compared for different delivery models and reflected in a business case that might incorporate cloud services.

Figure 4 shows some examples of IT service delivery strategies, incorporating cloud computing and some of the key considerations.
Preparing to revert might be one of the last things on the minds of business managers when engaging cloud services, but it is often one of the most important things to think about. The Satyam collapse\(^1\) a few years ago illustrates how a service provider may outwardly seem fine, but can unpredictably be brought down by unforeseen circumstances. Such situations are hard to predict, let alone prevent, and when relying on obscured cloud services, the uncertainty and risks can seem even greater. Businesses need to prepare themselves for what to do if and when a cloud provider fails. That is, they need a revert strategy to ensure that they can readily switch to a different IT service model at any time. This includes:

- Maintaining knowledge of all critical information and processing assets held in the cloud
- Maintaining sufficient skills (in-house or with a vendor independent of the provider) to be able to repatriate and reestablish systems and services

Revert strategies cost time and money, but they are important to mitigating the risk of a cloud provider failing. Additionally, they put cloud customers in a much stronger position when renegotiating a cloud service contract or with an independent vendor for a period (potentially even with another cloud provider)

<table>
<thead>
<tr>
<th>Service Model Examples Using Cloud Computing</th>
<th>Key Benefits</th>
<th>Key Risks to Consider</th>
</tr>
</thead>
</table>
| 1. Operate the entire production application using public cloud-based PaaS or SaaS, including customer interface, data transmission, processing and storage. | - Significantly lower operation and support costs  
- Potentially more reliable and resilient service than on-premise model  
- Reduced exposure to site-specific threats (e.g., disaster) by use of distributed sites  
- Services rapidly scalable, as and when required  
- Better able to avoid future risks of end-of-life architecture and technological obsolescence | - Consider incident response and recovery arrangements in the event of loss of cloud service.  
- Consider protection of data in the cloud, such as by encryption.  
- Consider other measures to protect the security of cloud-based assets and services.  
- Consider strategies to revert or to switch providers if needed. |
| 2. Operate the production environment using traditional on-premise servers, and use cloud IaaS for development, test and failover/recovery environments. | - Reduced costs of maintaining redundant environments that are only in use periodically  
- Better service quality through the ability to scale for volume and stress testing and/or recovery during peak processing times | - Consider data protection in the cloud when testing the use of live data or undertaking recovery activities. |
| 3. Operate the production environment using traditional on-premise servers, and use cloud IaaS for additional CPU and storage during periods of peak demand. | - Reduced costs of maintaining production capacity that is underutilized during nonpeak periods  
- Reduced capacity risks, as better able to scale up and down when peak processing demand is higher or lower than predicted | - Make similar considerations to scenario 1, although risks are limited to periods of peak demand processing. |
| 4. Use cloud IaaS or PaaS for developing new services during early release iterations, as features are evolving and demand is scaling. | - Greater flexibility in access to IT resources as services evolve and grow; less concern about acquiring resources that may become redundant later | - Consider risks regarding the security of intellectual property (e.g., software, algorithms) stored in the cloud.  
- Consider the increased criticality of incident response and recovery provisions as services scale. |

Regular backups of critical cloud-based assets held with facilities independent of the provider

Regular rehearsals, possibly by running services in-house or with an independent vendor for a period (potentially even with another cloud provider)

When in public, keep valuables under lock and key and stay alert—The need to protect sensitive data or intellectual property is particularly important when using a public cloud service. Typically, the best way to protect these assets is to use encryption technologies. In recent years, encryption has become more readily available, inexpensive and easier to setup, but it is complex, and there are many aspects to consider. Here are a couple key points to be aware of:

- Protecting data at rest and in transmission in the cloud can be readily achieved using encryption, but protecting data during processing in the cloud is problematic. Essentially, this is because when data are decrypted for processing, they are at risk, even if for a nanosecond. Basically, most
businesses wishing to perform processing on sensitive data in the cloud would be best advised not to use a public cloud model.

- Encryption is only as strong as the key management practices used around it. Many businesses have struggled to establish good processes for creating, distributing and renewing encryption keys. With a move to the cloud, where distribution of keys may be even greater, getting these processes in place becomes even more critical. Businesses not accustomed to implementing key management practices would be well advised to seek expert advice.

Businesses need to use encryption and stay alert. With traditional IT services, use of intrusion detection, alerting and prevention techniques has become common. But in terms of moving to the cloud, many of these tools are now in the hands of cloud providers, who may use these techniques to protect their networks and servers from attack. But, this does not mean that cloud providers will alert customers if a threat comes close to compromising customers’ assets. In fact, unless businesses tell cloud providers that they want to receive security-event alerts, cloud providers might assume that customers do not want to know.

Fortunately, many cloud providers offer their customers the ability to receive security-event alerts and even to flag the specific assets that they want to be monitored. Should a security event occur on a cloud provider’s network, businesses might still be reliant on the cloud provider to block an attack. They can, however, take their own evasive action to protect their assets, such as by bringing them offline.

KEEP THE LAW IN MIND WHEN TRAVELLING IN THE CLOUD

Before engaging with a cloud provider, there is another major area that warrants consideration: legal and regulatory requirements. In the old (pre-European Union [EU]) days of pan-European train travel, every time a train reached a border, government officials would come on board and check passenger passports before passengers could proceed. And, just because passengers purchased tickets to a particular destination did not mean that they would be allowed to get there if they did not have the right visas, for example.

The cloud can operate similarly. Just because a business purchases a service that operates across data centers around the globe does not mean that the business is allowed to send its data around the globe. Data privacy and sovereignty laws and requirements have sprung up around the world over recent decades. If businesses handle data covered by these requirements, they need to travel in the cloud with great care, or risk breaching the requirements.

Adherence to these laws and regulations can be complex, as there are many gray areas and legally untested situations, such as what constitutes export of data. The best recommendation is to obtain legal advice before entering into any cloud arrangements, particularly when operating in heavily regulated industries, such as financial services or health care, or where systems involve personally identifiable information (PII). In some cases, businesses may want to (or even be required to) consult with regulatory authorities directly.

For businesses subject to strict data-privacy or export laws, there are measures that can be put in place. For example, they can seek a cloud provider that offers geo-specific services, i.e., services in which operations are confined within certain jurisdictional boundaries.

Depending on the circumstances, there are many other areas of potential legal complexity, too. For example, what happens if an incident occurs in the cloud? Does the customer have the right to conduct a forensic investigation? Who will be liable for damages? Clearly, obtaining good legal advice is paramount for businesses to protect their rights and meet their obligations.

SELECTING A SERVICE PROVIDER—TRANSPARENCY AND TRUST

When it is time for a business to start evaluating service providers against its needs, there is a very important factor to consider: transparency. Cloud computing is much more than just buying IT hardware or software. It is about engaging a service that may be entrusted to manage critical assets and services, and there may be little day-to-day visibility of how this occurs. But, businesses can and should ensure a level of transparency.

With a traditional IT model (either on-premise or for many outsource arrangements), getting visibility is usually a case of commissioning an audit, either by internal auditors or by an outside party. But, for cloud services, this option is much less likely to be available or even practical, as the cloud service provider’s processing may be distributed throughout the world.

Therefore, alternative methods of gaining visibility of security and control will often be needed. There are several methods available, and, recognizing the need to establish trust, cloud providers are investing more and more in providing the information their customers need. This is an area that is likely to grow and evolve, and maybe one day a single common standard will be in place. However, in the meantime, here are some typical methods used by cloud providers to provide transparency. Each has pros and cons; therefore, often the best approach is to seek a combination of these:

- **Nondisclosure agreements**—Understandably, many cloud providers are protective of information about their architecture, security and controls. But, recognizing a prospective customer’s legitimate need to know these details, they will share limited information upon signing a nondisclosure agreement. If offered, this is definitely worth
taking because it will most likely shed valuable light on the provider’s services. However, it is important to bear in mind that this information may or may not have been independently verified.

- **Independent auditor reports**—Many service providers are now engaging independent auditors to assess the design and operation of their controls and to make these assessments available to their customers in the form of an independent audit report. Sometimes generically referred to as “SAS 70 reports,” there is a range of reports available. In the US, these include Statement on Auditing Standard (SAS) No. 70, Service Organization Control (SOC) 1, SOC-2 or SOC-3 reports, based on the American Institute of Certified Public Accountants (AICPA) standards. There are equivalent standards in other parts of the world.2

- **Certifications**—While independent audit reports are valuable, the scope and nature of controls can vary from provider to provider. One way to more easily compare providers is to look for industry certifications. Some of the more common and relevant certifications to look for are:
  - ISO 27001 and 27002 certifications provide assurance that the provider has implemented a set of security controls as well as a system of management practices to oversee the controls.
  - ISO 31000 certification means that the provider has established a framework and practices for managing its operational risks around delivery of its key services.
  - Payment Card Industry Data Security Standard (PCI DSS) compliance means that the provider has established security controls sufficient to enable credit card data to be stored, processed and transmitted using their systems. This requirement is quite stringent and valuable to a business that is looking to use a service for handling its sensitive information.

A note of caution: It is important not to take any audit report or certification at face value without examining its details. It is important to review its purpose, scope and any major exceptions, and to assess these against the business’s critical compliance, risk management and control needs.

**CONCLUSION**

Recently, news broke of Dropbox allegedly misleading customers regarding the levels of data protection provided by its service. This occurred shortly after Amazon’s EC2 service experienced major outages. With these and other events, media reports are asking, “Is this the end of the innocence of the cloud computing ideal?” The reality is that, as cloud services continue to grow and mature, there will be some derailments along the way. But the economics appear to be sound and compelling, and many of the technologies underpinning the cloud are maturing and proliferating quickly. So, it seems that cloud computing is an industry trend that is here to stay. That said, there are clearly a number of risks and uncertainties in transitioning to the cloud, so strong governance and control are an essential part of any decision to transition to the cloud.

But, for business managers who only glance at media headlines or skim glossy marketing materials, the path ahead may well be confusing and, at times, frightening. There are major opportunities here for IT governance and risk managers to educate and guide their business leaders on prudent ways to take advantage of the cloud. IT governance and risk managers can provide immense value in developing strategies that leverage the positive economic and risk-mitigation benefits of the cloud while also adopting control and assurance methods that help avoid the risks.

**REFERENCES**

Armbrust, Michael; et al; “Above the Clouds: A Berkeley View of Cloud Computing,” University of California at Berkeley, USA, February 2009


Wright, Dave; “Selecting a Hosting Partner for Your Software Plus Services Application,” Microsoft Communication Sector, August 2008

**ENDNOTES**

1 Kumar, Manoj; “Scandal at Satyam: Truth, Lies and Corporate Governance,” India Knowledge@Wharton, January 2009

2 A good comparison of the reports can be found at www.aicpa.org.