

Risk & Controls Solutions

Information Security
Services

Security among the Clouds



What would you like to change?

PRICEWATERHOUSECOOPERS 

Cloud computing is rapidly moving from hype to a must-have service model. The benefits are certainly real, but organisations must ensure that the cloud environment is secure enough for their essential data.

Table of contents



	Page
The heart of the matter	2
<p>Clouds on the horizon are bringing a fresh approach to IT services. The cloud computing model can help you achieve lower costs, reduced complexity and improved flexibility</p>	
An in-depth discussion	4
<p>Cloud computing offers clear benefits, yet its security risks are real. Chief information officers (CIOs) must fully understand both the inherent shortcomings and strengths of cloud computing to unlock its full potential and value.</p>	
The realities and risks of the cloud	7
How cloud service providers mitigate risk	9
The right data and applications for the cloud	10
Assess your risks – and the cloud provider’s capabilities	11
What this means for your business	14
<p>Cloud computing can bring increased efficiency to an organisation, but a successful implementation requires a new mindset—and new tools—to help ensure that security meets business needs.</p>	
Contacts	16

The heart of the matter

Cloud computing is a fresh approach to IT services that can result in lower costs, less complexity, and increased flexibility.

The heart of the matter



Cloud computing has been trumpeted as the biggest breakthrough since e-commerce. That assertion has yet to be proven, but clearly this new computing model is transforming the way IT services are provided, consumed and managed.

Cloud computing promises significant cost savings, diminished IT complexity, and increased flexibility in managing IT and responding to market changes. Is it a coincidence that these issues are also top of mind for today's CIOs?

Maybe not.

Unlike many technologies, cloud computing has evolved in response to customer needs for better, faster and cheaper methods of managing information technology. Indeed, individual customer demand defines the level of services, applications, storage and availability that the cloud delivers. Technology rarely evolves based purely on customer needs, but cloud computing appears to be an exception.

Cloud computing has multifaceted definitions as it relates to the many types of IT customers. For the line-of-business executive, cloud computing is a buyer-centric view of technology in which applications are available through purchase, rental, or development. For the chief financial officer, the cloud offers an approach to consume technology in a pay-as-you-go model that delivers the cost benefits of variable pricing without a costly investment in hardware. And for the CIO, cloud computing provides a comprehensive virtualisation model for technology that stretches from infrastructure design through application testing and delivery.

Combine them, and it's clear that cloud computing holds enormous potential for dramatic savings in operating costs and new efficiencies in delivery of IT services.

But let's not overlook the elephant in the room: security.

Information security keeps chief information security officers (CISOs) up at night, and with new computing models such as cloud computing, the stakes can be perilously higher. The possibilities of data loss, data leakage, downtime of service providers, regulatory breaches and risk of intellectual property theft create a treacherous risk environment.

These security issues illustrate the significant hurdles a business must clear before adopting cloud computing. Any organisation considering a move to the cloud must carefully assess what applications and data it can migrate to a cloud environment because cloud computing may not be appropriate for all business processes.

Organisations must also carefully examine the capabilities of any potential cloud services provider. Security, compliance, availability, and scalability are all factors that must be thoroughly evaluated using a comprehensive methodology. At the same time, it is important to consider the financial viability of the service provider. A business does not want a vendor to disappear the month after it moves its processes into the cloud.

In today's environment, adding value and increasing efficiency are imperative. Cloud computing has matured to the point that it can be a secure, viable and highly effective approach. But without careful planning and consideration of market concerns, the gains can be overshadowed by the risk exposure.

An in-depth discussion

Cloud computing offers clear benefits, yet its security risks are very real. You must understand both the inherent shortcomings and strengths of cloud computing to unlock its full potential and value.

An in-depth discussion



It has been a tough two years.

Few businesses, if any, have endured the ongoing global economic recession unscathed. Most are still struggling to reinvent processes and goals to ensure that their company is competitive and growing. To do so requires a new mindset—and a new technology—to cut costs and increase efficiencies.

PricewaterhouseCoopers believes cloud computing will be a prime choice for many businesses.

The adoption rate of cloud computing is soaring. Today 30 percent of respondents to a survey conducted by CIO Research said they are already using cloud computing. By 2012, 80 percent of Fortune 1000 enterprises will pay for cloud computing services, and 30 percent will pay for a cloud-computing infrastructure, according to Gartner Research¹. That same year, the technology will begin to reach mainstream critical mass and soon thereafter will become the preferred choice for the majority of application development efforts among large enterprises².

It's no wonder, then, that adoption of cloud computing is increasing as CIOs look beyond the hype and see that the technology has matured. It has been tested by large-scale implementations in business functions such as human resources and it has hosted functions such as e-mail. Another source of confidence is the growing presence of trusted players as service providers, including Amazon.com, Verizon Communications, EDS, Google, AT&T, IBM, and Microsoft. Recently, Microsoft unveiled a new cloud-computing platform called Azure.

Cloud services couldn't have matured at a more opportune time, as business leaders scramble to cut costs and increase agility. The cloud-computing model is cost-efficient because the company pays only for what it needs and uses. This variable cost structure enables the business to take advantage of up-to-the-minute technologies without a prohibitive up-front investment in hardware and software. The payoff looks promising.

The cloud model also can save money by recapturing the lost value of underutilised hardware. Infrastructure resources often lie idle in most organisations: PCs and servers, for instance, are used at only 10 percent of their processing capacity, while network storage is utilised at 50 percent capacity.

As hardware goes unused, software often becomes outdated. Many enterprise applications are proprietary, slow, and unable to communicate with other applications; they also exhibit single points of failure. Yet they are too expensive to replace. Cloud computing provides a shift to new applications with a pay-as-you-go pricing plan.

With cloud services, the service provider can scale or add applications on the fly to adjust to fluctuations in demand. For example, if a business needs a new application for monitoring customer support calls, a cloud service provider can quickly deploy the application without any need for the business to install and configure new hardware or software.

1. Gartner Symposium IT/Xpo, Cloud Computing Meets Data Center Realities, April 2008.

2. Gartner Research, Cloud Application Infrastructure Technologies Need Seven Years to Mature, Mark Driver, December 2008

An in-depth discussion (continued)



The cloud model also provides built-in redundancy with no single point of failure. Stress testing of major cloud vendors has increased resilience as well as the ability to provide high quality service level agreements, giving businesses flexibility while decreasing downtime. And cloud computing can enable in-network redundancy with automated recovery to help eliminate disaster recovery risks and costs.

The cloud model offers another critical step toward agility: full customer self-service. This enables businesses to provision, manage, and terminate services without involving the service provider. The result? Speedy, efficient management of IT services and functions.

The realities and risks of the cloud



The fear factor is often high when organisations consider any new technology that touches enterprise data and applications. It would help to be aware of the risks inherent in cloud computing.

The most public concern has been availability and reliability of services because outages can lead to operational downtime, resulting in lost revenue or a blemished reputation. Even large providers have experienced well-publicised service outages. These outages typically last less than an hour, but even brief downtime can disrupt a business's operations. Early this year, for instance, a 40-minute outage by one large service provider thwarted an estimated 177 million transactions around the world.

Many organisations fixate on privacy as a primary concern. Data privacy is complex because it is regulated in ways that vary by industry, by country, and even by state. Some CISOs fear that because data may be stored on shared servers, which span multiple geographies in an approach known as multi-tenancy, sensitive information could be governed by multiple, sometimes conflicting, jurisdictions. Compounding this risk are the decentralised support structures employed by the cloud service providers, which increase the risk that the same sensitive information may be viewed by unauthorised users or even competitors. This type of incident is rare, but it has been reported on at least two occasions when a large cloud service provider inadvertently shared user documents with others who had not been granted access to them.

Given the limited understanding of data flow in a cloud environment, data classification and data-handling practices employed by companies also concern CISOs. Indeed, in several incidents hackers have guessed user passwords to gain access to confidential documents stored in the cloud and then forwarded those documents to online news outlets. In other cases, cloud service providers simply lost customer data. This year, for instance, a bookmark-sharing website lost both its primary store of user data as well as its backup. In another case, an online-storage site shut down its service after losing nearly half its database of customer documents, photos and backups.

When data privacy is an issue, so too is compliance with regulatory mandates. Many of today's privacy regulations mandate where information must be stored or processed. The cloud model enables data to bounce swiftly around the world by using available server capacity in various geographic locations. Businesses now face new regulatory requirements that address where its data is physically stored and how it is accessed. The upshot? A German company with data residing in the United States is subject to both US and German privacy and security laws and regulations.

This level of regulatory complexity leads some organisations to believe that they are better off managing all their data in-house.

What's more, some organisations worry that a cloud service provider might go out of business. That is a valid concern given the rocky state of the economy, and that it has already occurred. This year, a cloud development provider shut its doors and gave its customers just a few months to remove all their applications and data.

However, a careful assessment of a company's needs and a cloud service provider's controls can help allay those concerns and possibly convince the company that in-house data storage is not the best option.

How cloud service providers mitigate risk



The reality and highly public profile of security lapses has not escaped the attention of top-tier cloud service providers. During the past two years, they have implemented critical controls and deployed technologies that aim to mitigate risks to reach a level of security that is trustworthy for critical data and applications.

In many cases, security has become a core competency that is fully integrated into the service. Cloud providers have developed suites of services designed to address cloud security on an end-to-end basis. These services, for instance, may include standard IT security tasks such as identity and access management, host-intrusion detection, application vulnerability assessment and network application assessment. They allow companies doing business in the cloud to treat security as a natural extension of their data network and, in some cases, to integrate security in the cloud with enterprise network security.

Similarly, cloud service providers offer security against traditional network attacks, including denial of service, IP spoofing and botnets. Many offer virtual firewalls, with an inbound firewall configured in a default-deny mode that requires the customer to open ports to allow inbound traffic. One vendor recently launched a web application firewall (WAF) provided as a service. A WAF is critical to many businesses because it's utilised to satisfy part of the Payment Card Industry Data Security Standard (PCI DSS) requirement.

Most suppliers encrypt data in transit and some encrypt data at rest. Those that do not encrypt data at rest may protect it by spreading the data across multiple machines so that a hacker cannot target a single server for attack.

One major cloud supplier has developed technologies that separate applications and data on the same infrastructure. The supplier also ensures the separation of workloads through the separation of the virtual machines and also the separation of client data in a shared database.

Finally, reliable vendors have undergone audits of controls around confidentiality, integrity and availability of the data on their systems. Cloud service providers may have ISO 27001 certification, which systematically examines the company's data security risks and then designs and implements a comprehensive suite of information security controls to address unacceptable risks.

In addition, some suppliers may have undergone an SAS 70 Type II audit, which requires an independent third party to verify that the proper controls are in place and operating effectively. Although there is no standard attestation method for cloud service providers, CIOs should require at least one of these two audits.

The right data and applications for the cloud



Cloud security has improved from its earliest stages, but that doesn't mean a business should consider the technology safe enough to house all of its sensitive data. Companies must assess their current infrastructure to determine what data and applications should—and should not—be outsourced to the cloud.

PricewaterhouseCoopers believes that any non-differentiating business function that can realise cost savings can benefit from cloud computing. This would include, for example, human resources, accounting, and customer relationship management (CRM). Hosted applications such as e-mail, web conferencing, and payroll are other areas in which cloud computing could lower costs help save money.

However, governance, mission-critical data and protected intellectual property should remain within the locked-down confines of the enterprise. It also may not be appropriate to put regulated data on the cloud. Data that require enhanced security measures, such as credit card information and healthcare records, should be sent to the cloud only if enterprise-level security controls are in place.

Before an enterprise moves data to the cloud, CISOs must determine whether personally identifiable information will be involved—and whether international regulatory requirements regarding export or transport controls are a concern.

For data that may be audited, the business must ensure that the cloud service provider has the technical capability to identify where, when, and how data is used. PCI auditors, for instance, will want to know where data is located, where it has been and whether it has been altered without record.

Assess your risks – and the cloud provider's capabilities



The amorphous structure of cloud computing leaves CIOs and CISOs with a daunting challenge: after the CIO determines what services to send to the cloud, the CISO's role is to determine what controls must be in place. Together, they must then assess what cloud service providers offer and their security capabilities, understand any gaps in protections, and, finally, select a provider.

Easily said, but certainly not easily done. As we mentioned, there is no standard attestation method or control framework for cloud computing. Nor is there a one-size-fits-all implementation strategy; the installation will be unique to each individual business. To gain confidence in a potential provider, we believe a business should perform due diligence using an accepted security control framework and consider using an independent adviser during the selection process.

A successful cloud implementation will ride on matching the organisation needs with the service provider's capabilities. Cloud vendors have not always been forthcoming in discussing their security measures because they consider them proprietary. That is changing, however, because the level of security has become a differentiating point.

To get started, the first thing to know is that a business must understand its risks before it can measure the potential benefits of cloud computing. Simply put, if a business doesn't know its risks, it will not be able to determine which supplier will best match its needs.

A good security program will include key controls to mitigate these business risks. With cloud computing, these controls are critical:³

- **Contractual agreements:** You own the data, so you must determine what rights and recourse you have for security breaches or incidents.
- **Certification and third-party audits:** Ensure that the provider has some form of accepted third-party review of security (ISO 27001 certification, for instance). If possible, you should seek independent reviews of their facilities and operations.
- **Compliance requirements:** Ensure that the supplier meets your compliance needs. A critical factor will be the geographic locations of the provider's servers and your data. Be aware of laws that impact your data in any country in which it may reside.
- **Availability, reliability and resilience:** Make sure you agree upon availability and reliability needs.
- **Backup and recovery:** In the event of disaster, agree on recovery requirements; understand a provider's capabilities before you engage it.
- **Service levels and performance:** Agree on adequate service levels and know what recourse you have if performance does not meet these levels.
- **Decommissioning:** Ensure that data be securely deleted once the contract or service is terminated. This should include all backup copies on all storage media. Also make certain that the virtual machines or processes are also securely decommissioned.

3. The Open Security Architecture, Pattern: Cloud Computing, <http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing>

Assess your risks – and the cloud provider’s capabilities (continued)



In addition to these controls, organisations should implement additional information security controls (such as information rights management and data leakage prevention) to ensure that the data it wants to keep out of the cloud is not accidentally moved to the cloud. Businesses also should ensure that their incident response program is updated to address cloud incidents and that vendor agreements require the cloud providers to work with its customers during incidents.

The next step is to perform a “secure the cloud” analysis, a comprehensive risk-based evaluation of the cloud environment. This analysis will identify gaps in security measures that your business requires due to the unique attributes of your data or business processes.

The overall security assessment of a potential cloud environment, for instance, will include areas such as access management, security standards, information handling, patch management, and event monitoring and investigations. The goal is to identify gaps in security protections offered by cloud providers and to determine the most effective means to mitigate the risk to your data, including customising cloud services to your needs or extending your internal security governance measures to the cloud environment. Another goal is to understand potential ways data can be compromised and the likelihood that it will happen.

When assessing cloud service suppliers, organisations should apply risk ratings to the evaluation. In doing so, companies must pay particularly close attention to how well a supplier will be able to abide by their security policies. We believe that the best model is one in which all outsourced data is encrypted both in transit and in storage.

A “secure the cloud” approach should encompass the following:

- **Security:** The assessment of information security should include, at a minimum, data encryption, data storage location, segregation, risk management, user access, systems management and incident response.
- **Privacy:** Privacy assessed against a relevant generally accepted privacy principles audit framework.
- **Compliance of the highest risk areas:** An organisation must be certain that the cloud supplier can adhere to all its risk-management practices.
- **Scalability:** Scalability is assessed by due diligence on aspects such as load testing, stress testing and forecast growth.
- **Metering:** Metering can be assessed by revenue-recognition testing as well as due diligence on the integrity and security of metering systems.
- **Availability:** Availability can be measured by investigating resilience of the architectural components and reviews of data recovery and information retrieval aspects.
- **Data leakage:** The likelihood of data leakage can be examined by due diligence of a risk assessment of potential data-leakage considerations.

Businesses that are thinking about adopting a cloud model should consider the technology a part of their overall IT infrastructure, and include in it blueprint refresh, application rationalisation and outsourcing strategy. The cloud computing model continues to evolve rapidly, so today’s assessment may not be accurate within six months.

What this means for your business

Cloud computing can bring new levels of efficiency to an organisation, but a successful implementation requires a new mindset—and new tools—to help ensure that security meets business needs.

What this means for your business



Adoption of cloud computing is rapidly gaining momentum, and the cloud will become a mainstream solution in the next two years. PricewaterhouseCoopers believes that the cloud model promises new, more efficient ways to conduct business. We also believe that now is the time to begin a transition plan to move to the cloud.

Yet we recommend you proceed with caution.

Adopting cloud computing requires a new mindset, as well as new processes, skills and tools. Implementation of a cloud solution demands an analysis of your business needs, expected benefits and the capabilities of the cloud service provider. We believe an analysis of your business needs and the vendor selection are best undertaken with the assistance of a trusted partner with a strong strategic and technical vision. That is where we can help.

The cloud computing landscape is rapidly evolving, and PricewaterhouseCoopers can help you build data protection capabilities that align with the shifting realities of the cloud. We can perform a comprehensive “secure the cloud” assessment to match a company’s needs with a service provider’s offerings. Our team of specialists can help identify a service provider that is trustworthy, mature and capable of handling your sensitive data and production applications.

With cloud computing, information security is a particularly critical issue that requires highly skilled guidance in planning and implementation. PricewaterhouseCoopers is a recognised, trusted leader in security consulting with global expertise in the full range of data protection, privacy, and compliance solutions.

We bring discipline and rigour to the planning phases of the initiative. During the transition to the cloud solution, we provide strong business process knowledge to help organisations achieve a cost-effective transformation in both processes and technology.

Cloud computing heralds an evolution of business that promises to be as revolutionary as the emergence of e-business in the 1990s. We believe companies that embrace cloud computing in the next year can capitalise on early gains in cost and operational efficiencies.

Our advice? It’s time to get started on a new strategic path. One that reaches for the clouds.

Contacts



To have a deeper conversation on any of the topics mentioned, please contact:

Andrew Elsworth

Partner
National and Melbourne
Information Security Services Lead
+61 (3) 8603 6179
andrew.elsworth@au.pwc.com

Patrick Kevin

Executive Director
Canberra Information Security Services
+61 (2) 6271 9267
patrick.kevin@au.pwc.com

Malcolm Shackell

Partner
Sydney Forensics Technologies
Services Lead
+61 (2) 8266 2993
malcolm.shackell@au.pwc.com

Rich Sands

Senior Manager
Melbourne Information Security Services
+61 (3) 8603 2619
rich.sands@au.pwc.com

David Harley

Director
Brisbane Forensic Technology Services
+61 (7) 3257 8307
david.j.harley@au.pwc.com

Stephen Woolley

Partner
Melbourne Advisory - Consulting Services
+61 (3) 8603 3808
stephen.woolley@au.pwc.com

Jan Schreuder

Partner
Sydney Information Security
Services Lead
+61 (2) 8266 1059
jan.schreuder@au.pwc.com

Steve Ingram

Partner
Melbourne Forensics Technologies
Services Lead
+61 (3) 8603 3676
steve.ingram@au.pwc.com

Kim Cheater

Partner
Adelaide Information Security Services
+61 (8) 8218 7407
kim.cheater@au.pwc.com

Peter Quigley

Senior Manager
Sydney Information Security Services
+61 (2) 8266 3917
peter.j.quigley@au.pwc.com

Shane Devitt

Executive Director
Perth Information Security Services
+61 (8) 9238 3473
shane.devitt@au.pwc.com

pwc.com.au

