www.pwc.com/security

# *Navigating security in the cloud*

*Advisory Services*

*Security*

pwc

***Cloud computing is rapidly moving into the mainstream. The benefits are undeniable, but look at whether your security needs are met.***

# *Table of contents*

# *The heart of the matter*

Cloud computing has proved it can deliver lower IT costs, diminished infrastructure complexity, and enhanced flexibility. As the technology advances into the mainstream, organizations are finding that it also can spur innovation by lowering the financial barriers to creating new products and services.

Consider, for instance, a global pharmaceutical company. To rapidly investigate and develop new products, this drugmaker needed to quickly spin up computing burst capacity to run data – and processor-intensive algorithms for modeling, simulations, and visualizations.

After thoughtful consideration, the pharmaceutical company deployed select R&D environments to multiple cloud providers. The result? The cloud's on-demand, high-performance computing capabilities have enabled the company to rapidly deploy new test environments, which has dramatically reduced the cycle time from idea to execution. For instance, the company can provision a 64-machine cluster computer and complete a sequence set in 20 minutes – rather than 12 weeks – at a cost of less than $7. Rapid delivery of new computing environments has helped this pharmaceutical company's scientists make quick decisions on drug research and has significantly lowered the cost of innovation.

The drugmaker's experience illustrates a newfound power of cloud computing: A strategic ability to drive business growth, rather than simply delivering efficient IT services at a lower cost.

As the function of cloud computing expands, so does the need for effective security. Chief Information Security Officers (CISOs) understand that, while security for cloud computing is no different than security controls for any IT environment, the stakes can be perilously higher. This is because the possibilities of data loss, data leakage, service downtime, regulatory constraints, and risk of intellectual property theft are amplified in the cloud model.

Accordingly, significant security hurdles must be cleared before a business implements cloud computing. Organizations must first carefully assess which of its applications and data are appropriate to move to a cloud environment. The company also must strenuously evaluate the capabilities of any potential cloud services provider, including factors such as data security and privacy, compliance, availability, and scalability. At the same time, it is important to consider the portability of data and applications to ensure that organizations can move to a new provider should an existing vendor fail to deliver agreed-upon service levels.

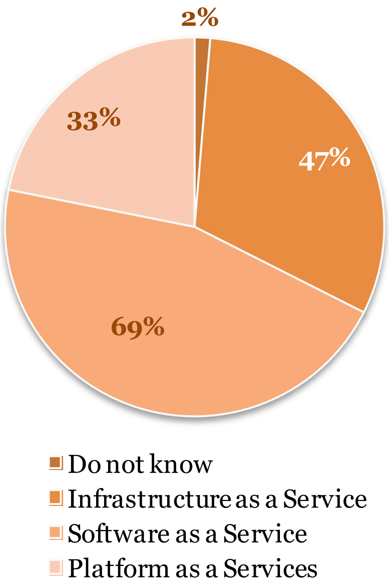
As cloud computing matures, organizations are beginning to understand that its benefits extend beyond lower IT costs and higher operating efficiencies. But without careful planning and consideration of market concerns, these gains can be overshadowed by risks.

# *An in-depth discussion*

Demand for cloud computing services has been fueled by the lingering effects of the global recession, which forced many organizations to trim costs while meeting increased customer demands. While this "do more with less" mandate remains a priority for most companies, many chief executives have turned their focus to growth – and to cloud computing.

**Saas leads cloud deployments**

41% of respondents to PwC's 2012 Global State of Information Security Survey say they have deployed some form of cloud computing. Most (69%) use Saas.



Today, business leaders recognize that the cloud presents a powerful new opportunity to drive business growth while meeting the challenges of cost containment. Its elastic architecture can spur innovation by lowering the financial barrier to trying new ideas and speeding the time to market for new products and services. Some companies, in fact, are using the cloud model to create new lines of business by partnering with external providers.

Given these benefits, it isn't surprising that cloud computing is evolving from experimental to mainstream. PwC's 2012 Global State of Information Security Survey of more than 9,600 security and IT leaders found that four out of 10 (41%) respondents said their business already uses cloud services. Adoption of the cloud is expected to skyrocket during this decade: Forrester Research forecasts that the global market for cloud computing services will soar from $40.7 billion in 2011 to more than $241 billion in 2020.[1]

One reason for this growth spike is the continuous maturity of cloud computing suppliers and trust of cloud service consumers. Tentative early implementations of cloud services have given way to large-scale deployments of business functions such as customer relationship management (CRM), talent management, payroll, and enterprise communications and collaboration.

Early implementations of cloud computing proved that the cloud's pay-as-you-go structure can trim IT spending and boost agility. It also allows a business to take

[1] Forrester Research, Inc., Sizing the Cloud, April 2011

advantage of up-to-the-minute technologies without prohibitive up-front investments in hardware and software.

The cloud model can save money by recapturing the lost value of underutilized hardware. Infrastructure resources often sit idle in most organizations: PCs and servers, for instance, are used at only 10% of their processing capacity, while network storage is utilized at 50% capacity.

**What's in a cloud? A definition**

Despite maturation of the industry, a precise definition of cloud computing remains somewhat elusive. To clarify, we will use the description published by the National Institute of Standards and Technology (NIST). The institute defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud solutions are typically marketed and described based on the type of services they deliver. Three of the most common offerings are:

- **Software as a service (SaaS):** The consumer employs a web browser to access a provider's applications running on a cloud infrastructure. (Examples: NetSuite, Salesforce.com, SuccessFactors)
- **Platform as a service (PaaS):** The consumer deploys applications on a cloud provider's infrastructure but has no control over the underlying network or servers. (Examples: Google App Engine, Microsoft Windows Azure, DotCloud)
- **Infrastructure as a service (IaaS):** The consumer provisions resources on the provider's infrastructure and can control operating systems, data, and applications – but not the underlying infrastructure. (Examples: Amazon.com EC2, Joyent, Rackspace.)

Cloud computing is commonly delineated by deployment model or service model. Today three deployment models are dominant:

- **Public:** A public cloud infrastructure is available to individual consumers or businesses.
- **Private:** A private cloud is operated solely for an organization and can be managed by the organization or a third-party company, on site or off site.
- **Hybrid:** A hybrid cloud comprises a mix of public and private cloud infrastructures that are discrete entities but are integrated to allow interoperability of data and applications.

With cloud services, hardware and applications are used (and paid for) on demand. The service provider can scale or add capacity on the fly to adjust to fluctuations in demand. As noted with the pharmaceutical company above, R&D computing resources can be deployed in a matter of minutes; the business need not install and configure new hardware or software.

The cloud model, if executed properly, also provides built-in redundancy with no single point of failure. Service level agreements (SLAs) that formally define expectations for issues such as availability, reliability, and performance can provide flexibility while decreasing downtime. Cloud computing also can enable in-network redundancy with automated recovery to help eliminate disaster recovery risks and costs.

The cloud model offers another critical step toward IT 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.

Finally, we are seeing new cloud solutions that empower employees to collaborate across departmental boundaries, which can improve knowledge sharing and efficiency in completing projects, and ultimately boost innovation.

## *The realities and risks of the cloud*

Any organization considering a move to the cloud must understand both the inherent shortcomings and strengths of cloud computing to reap its full potential and value.

Among CISOs, threats to data security and privacy have always been the dark side of the cloud. Yet as organizations adopt cloud computing, many are finding that security delivered by service providers meets or beats their needs. In fact, PwC's 2012 Global State of Information Security Survey found that 54% of companies that have implemented cloud computing report the technology has actually improved their security posture.

Advanced security capabilities implemented by service providers have persuaded corporations, non-profit organizations, and governments to entrust cloud service vendors with a widening array of data and applications.

There is perhaps no better indicator of this newfound trust than the US government's adoption of cloud-based solutions for several cabinet-level agencies, including the Department of Homeland Security, which is pursuing both public and private cloud solutions. In discussing their plans for cloud computing, government officials cite the cost savings of up to 10% and fast scalability of the cloud model, but they also tout the enhanced security of the cloud. [2]

At the same time, standards organizations are focusing on creating cloud security guidelines. The NIST and the Cloud Security Alliance (CSA), for example, have published new guidance and standards for cloud implementations.

Despite these advances, security leaders are most concerned about data privacy in the cloud. Our 2012 Global State of Information Security Survey found that 32% of respondents believe the greatest security risk is an uncertain ability to enforce the cloud provider security policies. Another worry, cited by 11% of respondents, is that data may be stored on servers shared with other companies. Because these servers can span multiple geographies, an approach known as multi-tenancy, sensitive information could be governed by multiple – and sometimes conflicting – jurisdictions.

CISOs also are well aware that the threat landscape today is unparalleled, with increasingly targeted – and effective – attacks perpetrated by sophisticated, patient intruders. The most serious of these threats originate from organized crime groups and nation states that have clandestinely launched a new generation of complex advanced persistent threats (APTs). At the same time, a growing movement of "hacktivists" representing loosely organized groups like Anonymous and LulzSec are also preying upon corporations and governments that run afoul of their political and social convictions.

[2] **Testimony of Richard A. Spires**, Chief Information Officer, before the House Committee on Homeland Security Subcommittee, October 6, 2011

Due to their sheer size, cloud-based service providers are tempting targets. Cyber criminals who gain access to a cloud data center can potentially steal millions of customer records, as well as valuable intellectual property and trade secrets. And because cloud providers often employ a multi-country infrastructure with servers and employees scattered across continents, the potential points of vulnerability are multiplied.

And it's not just hackers that keep security leaders awake at night. Employees of cloud providers, such as privileged system administrators and other "super users," may view or leak sensitive information, potentially damaging a customer's security posture and incurring costly reputational harm.

Similarly, insiders at a cloud consumer can unwittingly expose the organization to the same kinds of risk. Often, line of business managers purchase cloud services without the approval of IT or security leaders. These managers may mean well, but they are typically unaware of – and do not adhere to – security policies.

Another concern has been availability and reliability of services, since outages can lead to operational downtime that result in lost revenue or a blemished reputation. It's a hazard that even the most respected cloud providers have occasionally failed to avoid.

Data classification and data-handling practices employed by cloud providers 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 third parties. In other cases, cloud service providers simply lost customer data.

Another area of concern is data storage practices. The cloud model enables data to bounce swiftly around the world on leased servers in far-flung geographic locations. This can be enormously complicated for organizations that must comply with regulatory and privacy regulations mandating where information can be stored, processed, or accessed. A German company with data residing in the United States, for instance, is subject to both US and German privacy and security laws and regulations.

## *The right data and applications for the cloud*

Top-tier cloud service providers have implemented critical controls and deployed technologies to defend against these evolving threats. As cloud security continues to mature, their efforts have gained the trust of security leaders and C-suite officers.

Nonetheless, any cloud implementation must be approached with great caution and strenuous assessment. Organizations must evaluate their current infrastructure to determine which sensitive data and applications should – and should not – be sent to the cloud.

PwC believes that moving non-differentiating business function to the cloud would incur minimum risk to the organization. This would include, for example, human resources, payroll, accounting, and CRM, as well as hosted applications such as e-mail and web conferencing.

Mission-critical data and intellectual property, however, should remain within the locked-down confines of the enterprise. Similarly, regulated data like credit card information and healthcare records should be sent to the cloud only if the cloud supplier has security controls that match or surpass those required by the organization and its regulators. It is imperative to remember that the business, and not the cloud services provider, is ultimately responsible for security and ownership of this data.

When developing a business case to send data or applications to the cloud, the business-unit leader should work with IT and security personnel to determine what data and applications are appropriate for cloud computing. It also will be necessary to factor in the costs of working with IT and security teams to perform initial and on-going assessments.

Organizations should develop a flexible, adaptable framework to manage emerging governance and compliance issues. CISOs should delineate risk thresholds by working with the service provider to create common controls that define who is responsible for risk, as well as which party owns responsibility for data in transit and data at rest.

Before an enterprise moves data to the cloud, CISOs must determine whether personally identifiable information will be involved and whether international regulatory laws regarding export or transport controls are a concern. To that end, the business must know what data are subject to regulations such as those included in the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, Payment Card International Data Security Standard (PCI DSS), and the Sarbanes-Oxley Act.

For data that may be subject to audit, the business must ensure that the cloud service provider has the technical capability to identify where, when, and how data are used. PCI auditors, for instance, will want to know where data is located, where it has been, and whether it has been accessed without record. HIPAA auditors, on the other hand, will require a firewall that doesn't allow outsiders to make application programming interface (API) calls to their compute and storage systems, among other requirements.

## Assessing the cloud provider's capabilities

Once the CIO and business leaders determine which services and data to send to the cloud, the CISO must implement the proper controls. Together, IT and security executives will then evaluate cloud service providers and their security capabilities, understand any gaps in protections, and, finally, select a provider.

Today there is no standard attestation method or control framework for cloud computing, nor is there a one-size-fits-all implementation strategy; deployment will be unique to each individual business. To gain confidence in a potential provider, a business should perform due diligence using an accepted security control framework; engaging an independent adviser to help with this assessment is advisable for many organizations.

Another option that is gaining favor among cloud consumers is the use of a cloud broker. A cloud broker can help IT and security leaders negotiate the relationship with cloud providers and manage the use, performance, and delivery of cloud services. In addition to helping organizations obtain and customize services, cloud brokers can also help tailor security capabilities.

Whether using a broker or approaching the cloud independently, the following controls are critical:

- **Contractual agreements**: You own the data, so determine what rights and recourse you have for security breaches or incidents. Because you have no control over the cloud provider's infrastructure, SLAs, contract requirements, and provider documentation play a more important role than in traditional IT environments.
- **Access controls:** The cloud provider should prove that it has implemented and enforces administrative controls to limit employee and partner/supply chain access to your information. It also should adequately investigate the background of employees who will have access to data.
- **Certification and third-party audits**: Verify that the provider has some form of accepted third-party review of security (Statement on Standards for Attestation Engagements 16 or ISO 27001 certification, for instance). If possible, seek independent reviews of their facilities and operations. (See sidebar.)
- **Compliance requirements**: Determine whether the supplier meets your compliance needs. A critical factor will be the geographic locations of the provider's servers; be aware of laws that impact your data in any country in which it may reside.
- **Availability, reliability, and resilience**: Enact agreements on measurable availability and reliability service levels. Understand your options if the provider does not meet agreed-upon levels.
- **Backup and recovery**: In the event of disaster, document recovery requirements are in writing; understand a provider's capabilities before you engage it.
- **Decommissioning**: Agree that data will be securely deleted once it is no longer needed. Also make certain that virtual machines or processes are securely decommissioned.
- **Portability**: Determine whether you can easily move data and applications to another cloud provider or migrate data and applications back to an on-premises environment, if necessary. Before selecting a cloud provider, make sure that it does not use specialized or proprietary technologies that would create vendor lock-in.

In addition, organizations should implement additional data security controls (such as information rights management and data leakage prevention) to ensure that sensitive data is not inadvertently moved to the cloud. Businesses also should update their incident response program to address cloud incidents, and ensure that vendor agreements require cloud providers to work with its customers during incidents.

# An in-depth "secure the cloud" assessment

The next step is to perform a comprehensive risk-based assessment of the cloud environment. This overall security evaluation should include factors 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 determine the most effective means to mitigate the risk to your data, including customizing cloud services to your needs or extending internal security governance measures to the cloud environment. A secondary objective is to understand potential ways data can be compromised and the likelihood that it will happen.

### A new standard for independent assessments

Independent certification of cloud supplier capabilities is an uncertain undertaking because a comprehensive framework to measure cloud suppliers' capabilities does not yet exist.

Typically, cloud providers offer self- or third-party assessment using independent control frameworks like SAS 70 Type 2 reports. The SAS 70 auditing statement has been widely used to certify cloud providers, although it was not designed for this purpose.

SAS 70 has been replaced by the Statement on Standards for Attestation Engagements 16 (SSAE 16). Despite minor differences, neither extends beyond controls relevant to financial reporting.

Other assessment options include the Federal Information Security Management Act (FISMA) and ISO 27001. These standards focus primarily on traditional security issues, however, and do not include cloud concerns such as SLAs and multi-tenancy.

The American Institute of Certified Public Accountants (AICPA) has released a new standard for assessment of cloud service providers. The AICPA's Service Organization Controls (SOC) reports create an attestation standard designed to address broad control considerations, including security, privacy, availability, confidentiality, and processing integrity. SOC reports allow third-party auditors to report on operational and compliance controls that are relevant to cloud services.

When assessing cloud service suppliers, you should apply company-specific risk ratings to the evaluation. In doing so, pay particularly close attention to how well a supplier will be able to follow the letter of your security policies. We believe that the best model is one in which all outsourced data are 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 can be assessed using the generally accepted privacy principles audit framework published by the American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants. Organizations should also use the privacy guidance that is appropriate to their industry, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act.

- **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 unauthorized disclosure of data can be examined by a risk assessment that specifically evaluates data-leakage vulnerabilities.

While businesses have no single official framework for attestation of cloud providers, the US government has developed an authorization framework as part of its Cloud First initiative. The framework, known as the Federal Risk and Authorization Management Program (FedRAMP), provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services

This unified certification program was designed to achieve consistent security authorizations using agreed-upon standards and accredited third-party assessment organizations. All new cloud service providers must comply with this framework, which is largely based on existing FISMA controls. Cloud vendors that are already doing business with government agencies must attain FedRAMP compliance within two years.

The Department of Homeland Security (DHS) has primary responsibility for the FedRAMP initiative. A Joint Authorization Board, which comprises CIOs from the DHS, the Department of Defense, and the General Services Administration, reviews assessment results conducted by third-party organizations and grants authorization to service providers. Once authorized, a cloud service provider is recognized as meeting federal security requirements and can be employed by other agencies without an additional assessment. This “approve once and use many” approach is designed to help government agencies quickly and cost-effectively assess and engage providers.

FedRAMP illustrates the US government’s commitment to accelerate the adoption of cloud computing. Ultimately, FedRAMP will also increase confidence in the security and privacy of data stored on the cloud.

# *What this means for your business*

Cloud computing can transform the way you do business. Like any transformation, however, a successful cloud strategy requires a new mind-set – and new tools – to help ensure that security meets your specific needs.

If you haven't developed a cloud strategy, now is the time to start. Yet we urge you to include security controls and periodic security assessments in your strategy.

Implementation of a cloud solution demands a thorough analysis of your business needs, expected benefits, risks, and the capabilities of the cloud service provider. We believe this assessment is best undertaken with the assistance of a trusted partner with a strong strategic and technical vision. That is where we can help.

PwC can help you build data protection capabilities that align with the shifting cloud environment. We can perform a comprehensive "secure the cloud" assessment to match your 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, data security is a particularly critical issue that requires highly skilled guidance in planning and implementation. PwC is a recognized, trusted leader in security consulting with global expertise in the full range of data protection, privacy, and compliance solutions.

The benefits of cloud computing are undeniable. We believe it's time to get started on a new strategic path. One that stretches to the clouds.

# Contacts

To have a deeper conversation on cloud computing security or on any of the topics mentioned, please contact:

| | |
|---|---|
| Gary Loveland<br>Principal, National Security Leader<br>gary.loveland@us.pwc.com | John Hunt<br>Principal, Washington<br>john.d.hunt@us.pwc.com |
| Brad Bauch<br>Principal, Houston<br>brad.bauch@us.pwc.com | Jerry Lewis<br>Principal, Dallas<br>jerry.w.lewis@us.pwc.com |
| Rik Boren<br>Partner, St. Louis<br>rik.boren@us.pwc.com | Mark Lobel<br>Principal, New York<br>mark.a.lobel@us.pwc.com |
| Kevin Campbell<br>Partner, Atlanta<br>kevin.campbell@us.pwc.com | Sloane Menkes<br>Principal, Washington<br>sloane.menkes@us.pwc.com |
| Michael Compton<br>Principal, Detroit<br>michael.d.compton@us.pwc.com | Joe Nocera<br>Principal, Chicago<br>joseph.nocera@us.pwc.com |
| Shawn Connors<br>Principal, New York<br>hawn.joseph.connors@us.pwc.com | Chris O'Hara<br>Principal, San Jose<br>christopher.ohara@us.pwc.com |
| Scott Evoy<br>Principal, Boston<br>scott.evoy@us.pwc.com | Fred Rica<br>Principal, New York<br>frederick.j.rica@us.pwc.com |
| Joe Greene<br>Principal, Minneapolis<br>joe.greene@us.pwc.com | Sohail Siddiqi<br>Principal, San Jose<br>sohail.siddiqi@us.pwc.com |
| Peter Harries<br>Principal, Phoenix<br>peter.harries@us.pwc.com | Andy Toner<br>Principal, New York<br>andrew.toner@us.pwc.com |

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.