Protecting your brand in the cloud
Transparency and trust through enhanced reporting

Third-party Assurance

November 2011

At a glance

Cloud computing has unprecedented potential to deliver greater business agility and flexibility while lowering IT costs.

Concerned about the risks of cloud computing, large enterprises have been cautious about adopting a holistic cloud computing solution.

Third-party assurance has the potential to deliver the insight companies need to move to the cloud with confidence.

pwc

Introduction

Greater insight into cloud provider controls and capabilities could help accelerate the move to cloud computing.

Establishing trust in cloud computing

Companies that do business in the cloud or are considering cloud-based business models remain concerned about security—and are raising their eyebrows about service availability and data privacy. These companies are making business decisions based on cloud providers' ability to provide a secure, stable environment at a lower cost. Cloud providers, security vendors, integrators, and consultants all have an important role to play to meet the increasingly rigorous needs of their customers, industry groups, and regulators.

IT is experiencing a radical transformation—the movement of software, platforms, and infrastructure to the cloud. Cloud computing is changing the way businesses think about virtually every aspect of IT. In the simplest terms, cloud computing enables businesses to extend their storage and processing abilities through the Internet in ways not practical, efficient, or conceivable a few years ago. It is opening doors to new ways of offering services, sharing information, analyzing data, reaching customers, and structuring organizations.

In-house IT costs go down even as business flexibility increases thanks to the on-demand nature of cloud computing. Increasingly, cloud computing is becoming a foundation for business benefits well beyond IT cost savings—business agility fueled by rapid technology innovations is enabling the digital transformation of processes.

The cloud sounds irresistible. So why aren't more companies rushing to get there? In an era where corporate governance, compliance with regulations, and meeting stakeholder commitments are essential to a company's reputation, many business leaders are concerned about how they will address the issues that surface in every conversation about the cloud: *security, availability, data privacy and integrity, and compliance.*

In the past, as companies invested in IT, they invested in the people, processes, and controls necessary to protect their business against new risks associated with technology and automation. Moving to the cloud can provide unprecedented benefits, but it means giving up control over these risks. While businesses can outsource their systems, applications, and processes, they can't outsource their obligations—to investors, employees, customers, partners, and regulators—to manage risks. Companies must still:

- Protect shareholder investments
- Maintain high product and service standards
- Ensure the confidentiality and privacy of employee, customer, and partner data
- Meet compliance requirements

Meeting these commitments is vital to maintaining a company's brand and reputation. A slip could lead to disgruntled customers, costly fines, and negative press coverage, ultimately damaging a company's brand. Faced with their obligations and the risk of a potential threat to their brand, companies need transparency into how well cloud providers' environments address their concerns.

Third-party assurance—that is, independent reporting solutions to address the trust gap between providers and users—may be part of the answer. With third-party assurance, an independent and objective organization delves into a cloud provider's environment to identify, test, and disclose controls that govern the ability to deliver promised levels of service—and sufficient security, availability, data privacy and integrity, and compliance. Third-party assurance has the potential to be more than just a report on controls. It may be the catalyst companies need to embrace cloud computing with greater confidence.

Risks with cloud computing

In recent years, companies have shed non-core functions, freeing management, staff, and resources to focus innovation, growth, and productivity in the core business. Cloud computing extends that trend. Today, even more of the value of your company resides not in your infrastructure, but in the trust customers, partners, and other stakeholders place in you. Yet in moving to the cloud, you reduce your ability to protect your business from a variety of risks.

With cloud computing, risks include:

- **Security:** In a recent survey on enterprise security, 32% of respondents cited their inability to enforce provider security policies as the greatest risk to their cloud computing strategies.[1] You could be at a competitive disadvantage or subject to negative publicity and legal or regulatory action if your intellectual property or other data could be accessed by other cloud users. The same is true for data viewed and misused by cloud administrators.
- **Availability:** Cloud providers promise certain levels of availability and uptime, but you have no way of knowing if a provider has adequately prepared for high usage levels across multiple cloud users. This is an especially relevant concern for companies considering moving high-volume, data intensive, or critical transaction processing to the cloud.
- **Data integrity:** You rely on data to forecast, report on, and manage your business. Inaccurate or incomplete data coming from a cloud provider's systems could result in poor forecasting or incorrect public reporting. Your business may also be subject to regulations or legal processes that require ready access to significant historical data. Without sufficient data retention and access rights, you may be subject to fines, penalties, or judgments for noncompliance. Finally, your cloud service provider may use your data for secondary purposes if data ownership rights are not addressed in contracts.
- **Data privacy:** You are obligated to protect customer's and employee's personal data, such as Social Security numbers, health information, and credit card numbers, from breaches. Even the loss of relatively small amounts of customer data has led to bad publicity and brand damage for many large organizations. Exposing customers' personal information can also result in fines.

Cloud computing provides very clear benefits. However, these advantages require that your organization cede control over risk mitigation and management to a third-party cloud services provider. Moving to the right cloud provider can help your company save money, provide new services and products to customers, respond more quickly to internal IT needs, and expand dynamically as business grows. The question for your company is this: How do you choose the right cloud provider—one that will help you realize business objectives, while reducing risk and providing the trust and transparency you need?

1 PwC 2012 Global State of Information Security Survey

Responses to concerns fall short—but are gaining traction

Cloud providers know that businesses have reservations about cloud computing, but their efforts to overcome doubts often fail to inspire the confidence of potential cloud users. Customers and prospective customers are looking for timely, useful information with enough relevance and detail to help them make decisions and compare providers. They also want proof that a cloud provider is operating in a way that meets the changing regulations and standards set out by government agencies, industry groups, and their own governance boards.

Providers often try to address user concerns with:

- **Self-assessments:** Providers prepare assessments based on arbitrary frameworks, generally focused on the documentation of security policies. Even when these assessments are thorough, they are not objective.
- **Compliance "certifications":** Increasingly, customers are requiring providers to demonstrate compliance with a growing number of traditional standards, primarily focused on security. As a result, cloud providers are investing great amounts of time, resources, and effort into compliance with ISO 27001/27002, the Federal Information Security Management Act (FISMA), the Health Information Portability and Accountability Act (HIPAA), PCI Data Security Standards (PCI DSS), and other standards.
- **Customer audits:** Providers complete customer-prepared checklists and detailed questionnaires about capabilities, but a provider's need to protect confidential processes can limit the scope of customer audits. Also, cloud users need specialized resources to conduct effective audits.
- **Service level agreements (SLAs):** These agreements spell out the provider's obligations, but they often do not include customer-centric monitoring of SLA performance or financial adjustments for non-performance that protect cloud users.
- **SSAE 16 (replaces SAS 70) reports:**[2] These reports address a provider's internal controls as they relate to information processing systems that support financial reporting. But cloud computing risks go beyond those relevant to financial reporting, so while the SSAE 16 delivers insight, it is not sufficient to address the full scope of risks associated with cloud computing.

2 The Statement on Standards for Attestation Engagements 16 (SSAE 16) replaced the Statement on Auditing Standards No. 70 (SAS 70) in 2011 as the standard for service organization control assurance, for controls relevant only to financial reporting.

Protecting against risks with an independent perspective

Many cloud providers have invested heavily to develop highly secure and available environments. Yet every cloud provider is different. The technologies and processes used to deliver cloud computing are evolving, and there are no established technology or compliance standards. In the race to offer services ahead of the competition, some providers may cut corners or be dependent on less advanced architectures. To choose a provider you can trust, you need transparency into how providers' environments protect you from risk.

Third-party assurance has the potential to bridge the trust gap between you and cloud providers. Third-party assurance over the cloud calls for a reporting solution that covers areas of concern that extend well beyond the traditional financial reporting needs of users of service organizations addressed by SSAE 16. Independent and objective reporting over the controls that address security, privacy, availability, and data integrity would help you decide whether a provider can deliver the level of protection against risks necessary for your business.

Standard-setting organizations are beginning to respond to the challenges posed by the cloud environment. The American Institute of Certified Public Accountants (AICPA) recently released guidance designed to enhance providers' and users' understanding of existing standards service organization control reporting which can be applied to cloud service providers, as summarized in Figure 1.

The AICPA's Service Organization Control (SOC) reports may provide an opportunity that represents greater consistency, transparency, and comparability for cloud providers and their customers in the near term.

Leading companies will look at SOC 2 not as the finish line, but as the foundation for developing a flexible, agile attestation architecture. They will perhaps look to leverage the underlying attestation standards, specifically "AT 101", to develop integrated compliance reporting that will allow them to simultaneously address controls reporting for a variety of other compliance requirements, such as ISO 27001/27002, FISMA, HIPAA, PCI DSS, and other standards.

None of these compliance and regulatory frameworks was developed to address the issues unique to the cloud. Therefore, forward-thinking companies will also incorporate emerging control standards from organizations such as the Cloud Security Alliance, a newly formed, volunteer-driven group that is defining new standards for businesses operating in the cloud.[4]

AICPA Service Organization Reports (SOC)	*Description*
SOC 1	This is SSAE 16, a direct replacement for SAS 70. It focuses on internal controls over financial reporting. Designed primarily for auditor-to-auditor communications. Not intended to address non-financial reporting-related controls.
SOC 2	This is an assessment covering technology-related areas of primary interest to service providers and users, such as privacy, availability, confidentiality, processing integrity, and security. It is aligned to AICPA's Trust Services Principles and Criteria.[3] Reports allow for detailed descriptions of auditor's tests and results, similar to those in SOC 1.
SOC 3	This is a technology-focused assessment that is designed to provide an opinion on a service provider's adherence to the AICPA Trust Services Principles and Criteria. The report does not include information about the provider's service, controls, or tests by the service auditor.

3 The AICPA Trust Services Principles and Criteria reflect five principles and related criteria for controls that address the following areas: security, privacy, availability, confidentiality, and processing integrity. These five principles conceptually address most, if not all, concerns of cloud users.

4 Refer to the Cloud Security Alliance's "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0." For more considerations about risk, assessments, and security from a cloud perspective, see the European Network and Information Security Agency (ENISA) whitepaper "Cloud Computing: Benefits, Risks and Recommendations for Information Security," and ISACA's "IT Control Objectives for Cloud Computing."

Benefits to cloud providers

Third-party assurance does more than just serve the needs of cloud users. Cloud providers benefit as well, especially early adopters of third party assurance. By engaging with a qualified third-party, cloud providers can obtain a more comprehensive evaluation of their environment, as viewed through the eyes of their customers, and identify and address weaknesses. This will further improve their ability to gain customer confidence. And by giving potential customers an independent report, cloud providers can capture more business from cautious companies—and reduce reliance on time-consuming one-to-one reporting during the sales process.

Third-party assurance will help you understand a cloud provider's controls in any or all of the following areas:

- Security policies and procedures, including encryption, identification, authentication, and access management capabilities
- Availability procedures, monitoring, and resolution to ensure systems or services meet minimum performance levels for availability according to SLAs
- Ability to fulfill relevant compliance requirements
- Data privacy and integrity

Armed with a third-party report, you gain the insight you need to make the right choice for your business. You will be better prepared to confidently rely on a cloud provider to not only reduce the burden of maintaining internal IT, but also to maintain a reliable control environment. Third-party assurance may not become a standard practice overnight. But by seeking out cloud providers that do make independent assessments available, you may be able to trust your most valuable asset—your brand—to cloud computing more confidently.

www.pwc.com

To have a deeper conversation about any of the issues in this paper, please contact:

Cara Beston
+1 (408) 817-1210
cara.m.beston@us.pwc.com
San Jose, California

Joe Krull
+1 (210) 421-8233
joe.krull@us.pwc.com
Houston, Texas

Yonesy Nunez
+1 (646) 471-6531
yonesy.f.nunez@us.pwc.com
Philadelphia, Pennsylvania

Eric Tan
+1 (408) 817-7986
eric.tan@us.pwc.com
San Jose, California