An ISACA
Emerging Technology
White Paper

ISACA®
Serving IT Governance Professionals

Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

Abstract
Globalization and recent economic pressures have resulted in increased requirements for the availability, scalability and efficiency of enterprise information technology (IT) solutions. A broad base of business leaders has become increasingly interested in the costs and the underlying technology used to deliver such solutions because of their growing impact on the bottom line. Many parties claim that "cloud computing" can help enterprises meet the increased requirements of lower total cost of ownership (TCO), higher return on investment (ROI), increased efficiency, dynamic provisioning and utility-like pay-as-you-go services. However, many IT professionals are citing the increased risks associated with trusting information assets to the cloud as something that must be clearly understood and managed by relevant stakeholders. This paper clarifies what cloud computing is, identifies the services offered in the cloud, and also examines potential business benefits, risks and assurance considerations.

ISACA®

With more than 86,000 constituents in more than 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®) and Certified in the Governance of Enterprise IT® (CGEIT®) designations.

ISACA developed and continually updates the COBIT,® Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfill their IT governance responsibilities and deliver value to the business.

Disclaimer

ISACA has designed and created *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives* (the “Work”), primarily as an educational resource for security, governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security, governance and assurance professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Reservation of Rights

© 2009 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

CGEIT is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

ISACA wishes to recognize:

Project Development Team

Jeff Spivey, CPP, PSP, Security Risk Management, Inc., USA, Chair
Phil Agcaoili, CISM, CISSP, Dell, USA
Joshua Davis, CISA, CISM, CIPP, CISSP, Qualcomm Inc., USA
Geir Arild Engh-Hellesvik, Ernst & Young AS, Norway
David Lang, CISA, CISM, CISSP-ISSMP, CPP, PMP, Dell, USA
H. Peet Rapp, CISA, Rapp Consulting, USA
Jim Reavis, Cloud Security Alliance, USA
Ben Rothke, CISA, CISM, CGEIT, BT Global Services, USA
Joel Scambray, CISSP, Consciere, USA
Ward Spangenberg, CISA, CISSP, QSA, IOActive, USA

ISACA Board of Directors

Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President
Yonosuke Harada, CISA, CISM, CGEIT, CAIS, InfoCom Research, Inc., Japan, Vice President
Jose Angel Pena Ibarra, CGEIT, Alintec, Mexico, Vice President
Ria Lucas, CISA, CGEIT, Telstra Corp., Australia, Vice President
Robert Stroud, CGEIT, CA Inc., USA, Vice President
Rolf von Roessing, CISA, CISM CGEIT, KPMG Germany, Germany, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Lynn Lawton, CISA, FBCS, CITP, FCA, FIIA, KPMG LLP, UK, Past International President
Everett Johnson, CPA, Deloitte & Touche LLP (Retired), USA, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Director
Jeff Spivey, CPP, PSP, Security Risk Management, Inc., USA, Trustee

Guidance and Practices Committee

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Chair
Phil James Lageschulte, CGEIT, CPA, KPMG LLP, USA
Mark A. Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA
Adel H. Melek, CISA, CISM, CGEIT, Deloitte & Touche, Canada
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA, Capco IT Service India Pvt Ltd., India
Anthony P. Noble, CISA, Viacom, USA
Salomon Rico, CISA, CISM, CGEIT, Galaz, Yamazaki, Ruiz Urquiza, S.C., Mexico
Eddy Justin Schuermans, CISA, CGEIT, ESRAS bvba, Belgium
Frank Van Der Zwaag, CISA, CISSP, Westpac, New Zealand

The Cloud Security Alliance—for which ISACA is a founding member

Impacts of Cloud Computing

As CxOs search for ways to meet ever-increasing IT demands, many are closely examining cloud computing as a real option for their enterprise needs. The promise of cloud computing is arguably revolutionizing the IT services world by transforming computing into a ubiquitous utility, leveraging on attributes such as increased agility, elasticity, storage capacity and redundancy to manage information assets. The continued influence and innovative use of the Internet has enabled cloud computing to utilize existing infrastructure and transform it into services that could provide enterprises both significant cost savings and increased efficiency. Enterprises are realizing there is a potential to leverage this innovation to better serve customers and gain business advantage.

By offering enterprises the opportunity to decouple their IT needs and their infrastructure, cloud computing has the likely ability to offer enterprises long-term IT savings, including reducing infrastructure costs and offering pay-for-service models. By moving IT services to the cloud, enterprises can take advantage of using services in an on-demand model. Less up-front capital expenditure is required, which allows businesses increased flexibility with new IT services.

For all these reasons, it is easy to see why cloud computing is an attractive potential service offering for any business looking to enhance IT resources while controlling costs. However, it should be noted that along with the benefits come risks and security concerns that must be considered. As IT services are contracted outside of the enterprise, there is added risk with increased dependency on a third-party provider to supply flexible, available, resilient and efficient IT services. While many enterprises are accustomed to managing this type of risk in-house, changes are required to expand governance approaches and structures to appropriately handle the new IT solutions and enhance business processes.

> **"The promise of cloud computing is arguably revolutionizing the IT services world by transforming computing into an ubiquitous utility."**

As with any emerging technology, cloud computing offers the possibility of high reward in terms of containment of costs and features such as agility and provisioning speed. However, as a "new" initiative, it can also bring the potential for high risk. Cloud computing introduces a level of abstraction between the physical infrastructure and the owner of the information being stored and processed. Traditionally, the data owner has had direct or indirect control of the physical environment affecting his/her data. In the cloud, this is no longer the case. Due to this abstraction, there is already a widespread demand for greater transparency and a robust assurance approach of the cloud computing supplier's security and control environment.

Once it has been determined that cloud services are a plausible solution for an enterprise, it is important to identify the business objectives and risks that accompany the cloud. This will assist enterprises in determining what types of data should be trusted to the cloud, as well as which services might deliver the greatest benefit.

Just What Is Cloud Computing?

One of the most confusing issues surrounding the cloud and its related services is the lack of agreed-upon definitions. As with all emerging technologies, the lack of clarity and agreement often hinders the overall evaluation and adoption of that technology. Two groups that have offered a baseline of definitions are the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance. They both define cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Another way to describe services offered in the cloud is to liken them to that of a utility. Just as enterprises pay for the electricity, gas and water they use, they now have the option of paying for IT services on a consumption basis.

The cloud model can be thought of as being composed of three **service models** (**figure 1**), four **deployment models** (**figure 2**) and five essential **characteristics** (**figure 3**). Overall risks and benefits will differ per model and it is important to note that when considering different types of service and deployment models, enterprises should consider the risks that accompany them.

Figure 1—Cloud Computing Service Models

Service Model	Definition	To Be Considered
Infrastructure as a Service (IaaS)	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party.	Options to minimize the impact if the cloud provider has a service interruption
Platform as a Service (PaaS)	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider	• Availability • Confidentiality • Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite) • Data ownership • Concerns around e-discovery
Software as a Service (SaaS)	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).	• Who owns the applications? • Where do the applications reside?

Figure 2—Cloud Computing Deployment Models

Deployment Model	Description of Cloud Infrastructure	To Be Considered
Private cloud	• Operated solely for an organization • May be managed by the organization or a third party • May exist on-premise or off-premise	• Cloud services with minimum risk • May not provide the scalability and agility of public cloud services
Community cloud	• Shared by several organizations • Supports a specific community that has shared mission or interest. • May be managed by the organizations or a third party • May reside on-premise or off-premise	• Same as private cloud, plus: • Data may be stored with the data of competitors.
Public cloud	• Made available to the general public or a large industry group • Owned by an organization selling cloud services	• Same as community cloud, plus: • Data may be stored in unknown locations and may not be easily retrievable.
Hybrid cloud	A composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)	• Aggregate risk of merging different deployment models • Classification and labeling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type.

Figure 3—Cloud Computing Essential Characteristics

Characteristic	Definition
On-demand self-service	The cloud provider should have the ability to automatically provision computing capabilities, such as server and network storage, as needed without requiring human interaction with each service's provider.
Broad network access	According to NIST, the cloud network should be accessible anywhere, by almost any device (e.g., smart phone, laptop, mobile devices, PDA).
Resource pooling	The provider's computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand. There is a sense of location independence. The customer generally has no control or knowledge over the exact location of the provided resources. However, he/she may be able to specify location at a higher level of abstraction (e.g., country, region or data center). Examples of resources include storage, processing, memory, network bandwidth and virtual machines.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned, in many cases automatically, to scale out quickly and rapidly released to scale in quickly. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering capability (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and customer of the utilized service.

As can be observed in the characteristics listed in **figure 3**, there are many approaches and nuisances to cloud computing. Benefits to the enterprise, as well as risks, will vary depending on the types of service and deployment models selected.

The Business Benefits of Cloud Computing

While the promise of financial savings is a very attractive enticement for cloud computing, quite possibly the cloud's best opportunity is for enterprises to streamline processes and increase innovation. It enables increasing productivity and transforming business processes through means that were prohibitively expensive before the cloud. Organizations can focus on their core business, rather than be concerned about scalability of infrastructure. Solving peak business demands for performance can be readily met by using cloud computing—translating into more reliable backup, more satisfied customers, increased scalability and even higher margins.

Some of the key business benefits offered by the cloud include:

- **Cost containment**—The cloud offers enterprises the option of scalability without the serious financial commitments required for infrastructure purchase and maintenance. There is little to no upfront capital expenditure with cloud services. Services and storage are available on demand and are priced as a pay-as-you-go service. Additionally, the cloud model could assist with cost savings in terms of wasted resources. Saving on unused server space allows enterprises to contain costs in terms of existing technology requirements and experiment with new technologies and services without a large investment. Enterprises will need to compare current costs against potential cloud expenses and consider models for TCO to understand whether cloud services will offer the enterprise potential savings.
- **Immediacy**—Many early adopters of cloud computing have cited the ability to provision and utilize a service in a single day. This compares to traditional IT projects that may require weeks or months to order, configure and operationalize the necessary resources. This has a fundamental impact on the agility of a business and the reduction of costs associated with time delays.
- **Availability**—Cloud providers have the infrastructure and bandwidth to accommodate business requirements for high speed access, storage and applications. As these providers often have redundant paths, the opportunity for load balancing exists to ensure that systems are not overloaded and services delayed. While availability can be promised, customers should take care to ensure that they have provisions in place for service interruptions.

© 2009 ISACA. All rights reserved.

- **Scalability**—With unconstrained capacity, cloud services offer increased flexibility and scalability for evolving IT needs. Provisioning and implementation are done on demand, allowing for traffic spikes and reducing the time to implement new services.
- **Efficiency**—Reallocating information management operational activities to the cloud offers businesses a unique opportunity to focus efforts on innovation and research and development. This allows for business and product growth and may be even more beneficial than the financial advantages offered by the cloud.
- **Resiliency**—Cloud providers have mirrored solutions that can be utilized in a disaster scenario as well as for load-balancing traffic. Whether there is a natural disaster requiring a site in a different geographic area or just heavy traffic, cloud providers say they will have the resiliency and capacity to ensure sustainability through an unexpected event.

The premise of the cloud is that by outsourcing portions of information management and IT operations, enterprise workers will be free to improve processes, increase productivity and innovate while the cloud provider handles operational activity smarter, faster and cheaper. Assuming this to be the case, significant changes to the existing business processes will likely be required to take advantage of the opportunities that cloud services offer.

> **"…by outsourcing portions of information management and IT operations, enterprise workers will be free to improve processes, increase productivity and innovate…"**

Risks and Security Concerns With Cloud Computing

Many of the risks frequently associated with cloud computing are not new, and can be found in enterprises today. Well planned risk management activities will be crucial in ensuring that information is simultaneously available and protected. Business processes and procedures need to account for security, and information security managers may need to adjust their enterprise's policies and procedures to meet the business's needs. Given the dynamic business environment and focus on globalization, there are very few enterprises that do not outsource some part of their business. Engaging in a relationship with a third party will mean that the business is not only using the services and technology of the cloud provider, but also must deal with the way the provider runs its organization, the architecture the provider has in place, and the provider's organizational culture and policies. Some examples of cloud computing risks for the enterprise that need to be managed include:

- Enterprises need to be particular in choosing a provider. Reputation, history and sustainability should all be factors to consider. Sustainability is of particular importance to ensure that services will be available and data can be tracked.
- The cloud provider often takes responsibility for information handling, which is a critical part of the business. Failure to perform to agreed-upon service levels can impact not only confidentiality but also availability, severely affecting business operations.
- The dynamic nature of cloud computing may result in confusion as to where information actually resides. When information retrieval is required, this may create delays.
- Third-party access to sensitive information creates a risk of compromise to confidential information. In cloud computing, this can pose a significant threat to ensuring the protection of intellectual property (IP) and trade secrets.
- Public clouds allow high-availability systems to be developed at service levels often impossible to create in private networks, except at extraordinary costs. The downside to this availability is the potential for commingling of information assets with other cloud customers, including competitors. Compliance to regulations and laws in different geographic regions can be a challenge for enterprises. At this time there is little legal precedent regarding liability in the cloud. It is critical to obtain proper legal advice to ensure that the contract specifies the areas where the cloud provider is responsible and liable for ramifications arising from potential issues.
- Due to the dynamic nature of the cloud, information may not immediately be located in the event of a disaster. Business continuity and disaster recovery plans must be well documented and tested. The cloud provider must understand the role it plays in terms of backups, incident response and recovery. Recovery time objectives should be stated in the contract.

Strategies for Addressing Cloud Computing Risks

These risks, as well as others that an enterprise might identify, must be managed effectively. A robust risk management program that is flexible enough to deal with continuously evolving information risks should be in place. In an environment where privacy has become paramount to enterprise customers, unauthorized access to data in the cloud is a significant concern. When embarking on an agreement with a cloud provider, an enterprise must take an inventory of its information assets and ensure that data are properly classified and labeled. This will help to determine what should be specified when drafting a service level agreement (SLA), any need for encryption of data being transmitted or stored, and additional controls for information that is sensitive or of high value to the organization.

As the link that defines the relationship between the business and the cloud provider, the SLA is one of the most effective tools the enterprise can use to ensure adequate protection of information entrusted to the cloud. The SLA will be the tool where customers can specify if joint control frameworks will be utilized and describe the expectation of an external, third-party audit. Clear expectations regarding the handling, usage, storage and availability of information must be articulated in the SLA. Additionally, requirements for business continuity and disaster recovery (discussed previously) will need to be communicated in the agreement.

Information protection will evolve as a result of a strong, comprehensive SLA that is supported by an equally strong and comprehensive assurance process. Structuring a detailed and complete SLA that includes specific rights to audit will assist the enterprise in managing its information once it leaves the organization and is transported, stored or processed in the cloud.

"In an environment where privacy has become paramount to enterprise customers, unauthorized access to information in the cloud is a significant concern."

Governance and Change Issues With Cloud Computing

The strategic direction of the business and of IT in general is the main focus when considering the use of cloud computing. As enterprises look to the cloud to provide IT services that have been traditionally managed internally, they will need to make some changes to help ensure that they continue to meet performance objectives, that their technology provisioning and business are strategically aligned, and risks are managed. Ensuring that IT is aligned with the business, systems are secure, and risk is managed is challenging in any environment and even more complex in a third-party relationship. Typical governance activities such as goal setting, policy and standard development, defining roles and responsibilities, and managing risks must include special considerations when dealing with cloud technology and its providers.

If not already part of the business's governance or system development life cycle process, the move to cloud computing essentially dictates that a company information security officer or director be included in all further governance and system development life cycle processes.

As with all organizational changes, it is expected that some adjustments will need to be made to the way business processes are handled. Business processes such as data processing, development and information retrieval are examples of potential change areas. Additionally, processes detailing the way information are stored, archived and backed up will need revisiting.

The cloud presents many unique situations for businesses to address. One large governance issue is that business unit personnel, who previously were forced to go through IT, can now bypass IT and receive services directly from the cloud. It is, therefore, paramount that information security policies address uses for cloud services.

© 2009 ISACA. All rights reserved.

Assurance Considerations for Cloud Computing

When faced with the paradigm change and nature of services provided through cloud computing, there are many challenges for assurance providers. What can be done to improve the assurance professional's ability to provide direct and indirect users of cloud computing with trust in the software services and infrastructure that make up the cloud?

Some of the key assurance issues that will need to be addressed are:

- **Transparency**—Service providers must demonstrate the existence of effective and robust security controls, assuring customers that their information is properly secured against unauthorized access, change and destruction. Key questions to decide are: How much transparency is enough? What needs to be transparent? Will transparency aid malefactors? Key areas where supplier transparency is important include: What employees (of the provider) have access to customer information? Is segregation of duties between provider employees maintained? How are different customers' information segregated? What controls are in place to prevent, detect and react to breaches?
- **Privacy**—With privacy concerns growing across the globe it will be imperative for cloud computing service providers to prove to existing and prospective customers that privacy controls are in place and demonstrate their ability to prevent, detect and react to breaches in a timely manner. Information and reporting lines of communication need to be in place and agreed on before service provisioning commences. These communication channels should be tested periodically during operations.
- **Compliance**—Most organizations today must comply with a litany of laws, regulations and standards. There are concerns with cloud computing that data may not be stored in one place and may not be easily retrievable. It is critical to ensure that if data are demanded by authorities, it can be provided without compromising other information. Audits completed by legal, standard and regulatory authorities themselves demonstrate that there can be plenty of overreach in such seizures. When using cloud services there is no guarantee that an enterprise can get its information when needed, and some providers are even reserving the right to withhold information from authorities.
- **Trans-border information flow**—When information can be stored anywhere in the cloud, the physical location of the information can become an issue. Physical location dictates jurisdiction and legal obligation. Country laws governing personally identifiable information (PII) vary greatly. What is allowed in one country can be a violation in another.
- **Certification**—Cloud computing service providers will need to provide their customers assurance that they are doing the "right" things. Independent assurance from third-party audits and/or service auditor reports should be a vital part of any assurance program.

> **"Cloud computing represents a rare opportunity to rework security and IT controls for a better tomorrow."**

The use of standards and frameworks will help businesses gain assurance around their cloud computing supplier's internal controls and security. At the time of writing, there are no publicly available standards specific to the cloud computing paradigm. However, existing standards should be consulted to address the relevant areas and businesses should look to adjust their existing control frameworks. Cloud computing represents a rare opportunity to rework security and IT controls for a better tomorrow. Many businesses will no doubt grab this opportunity to improve both efficiency and built-in security of their IT portfolio.

© 2009 ISACA. All rights reserved.

Conclusion

While cloud computing is certainly poised to deliver many benefits, information security and assurance professionals should conduct business impact analyses and risk assessments to inform business leaders of potential risks to their enterprise. Risk management activities must be managed throughout the information life cycle and risks should be reassessed regularly or in the event of a change.

Enterprises that have been considering the use of the cloud in their environment should calculate what cost savings the cloud can offer them and what additional risks are incurred. Once potential cost savings and risks are identified, enterprises will have a better understanding of how they can leverage cloud services. Business must work with legal, security and assurance professionals to ensure that the appropriate levels of security and privacy are achieved. The cloud is a major change in how computing resources will be utilized, and as such will be a major governance initiative within adopting organizations, requiring involvement of a broad set of stakeholders.

Additional resources related to cloud computing

© 2009 ISACA. All rights reserved.