

Cloud Computing *Examining the Risks of Virtualized Resources*



William Gallagher Associates
Phone: 888.261.8884
www.WGAins.com

The idea of cloud computing is designed around an architecture whose natural state is a shared pool outside an enterprise. It allows for accessibility via the internet, always available and scaled to demand, and is usually offered as a “pay as you use” feature. While all of this sounds attractive, the use of cloud computing unfortunately has some very real risks for security, privacy, compliance and data integrity.

The benefits of cloud computing are compelling, particularly for a start-up or small company that is confronted with a need to add significant IT infrastructure quickly. Utilizing the cloud services of *Amazon* or *Google* can eliminate a host of concerns and changes what is frequently a long term investment into an income statement expense. The subsequent freedom from long term leases or other financing mechanism provides real financial flexibility. Given these very favorable circumstances, it is quite tempting to maximize business usage of the cloud particularly in light of current economic climate.

Proceed well-armed and prudently

To give you a clear understanding of precisely why the cloud poses special risk, we suggest a thorough risk analysis during the decision process and using a detailed risk check list when and if you decide to enlist a cloud service provider.

What makes cloud computing unique and unlike traditional IT outsourcing, you frequently do not precisely know who is working with your data and where it is hosted. Cloud computing decouples data from the infrastructure and obscures operational details. Multitenancy on servers is the norm, where software runs on a vendor's servers for multiple client organizations (tenants). This is being referred to as SaaS (software-as-a-service).

“In a shared pool outside the enterprise, you don’t have any knowledge or control of where the resources run. So if you have a concern over data location, as an example, that may be a reason for not using the cloud,” said David Cearley, Vice President at Gartner Research and a leading authority on information technology.

Bruce MacDougall, AAI

William Gallagher Associates is a leading provider of insurance brokerage, risk management and employee benefits services to firms with complex risks, within industries that include technology, life sciences, financial risks, health care, aviation, energy, and environmental services.

WGA has offices in Boston, MA; New York, NY; Hartford, CT; Princeton, NJ; Columbia, MD; Atlanta, GA; and Paris France.

According to expert Geoffrey Moore of TCG Advisors, in a recent *InfoWorld* article title “The Dangers of Cloud Computing,” a good rule of thumb for moving functions from behind the firewall should be based on the following: Core vs. Context, and non-mission critical vs. mission critical. Simply put, **if it is context and non-mission critical, use the cloud**; if it is a core and mission critical function, it should never use the cloud. Moore describes *Core* as a process that contributes directly to sustainable differentiation in your business. *Context* is all other processes required to fulfill a company’s commitments to one or more of its stakeholders.

Risks

The cloud offers some very innovative and financially favorable services, but the dangers are real due to the fact companies do not have control over their data, and without control, there is always inherent risk.

In September 2008 SalesForce.com experienced a security breach from a “phishing” attack that allowed for 40,000 customers of SunTrust to have their e-mail addresses and other contact information stolen. Another case in February involved a breakdown at Google Docs when they inadvertently shared a series of documents with a large group of people, rather than the limited group authorized by the user. It was rectified over a two week period, but it highlights how easily a data breach can take place, even at with a trusted provider like Google.

Below is a list of risk management questions to help minimize risks during in the process of choosing a cloud computing provider:

Security

Physical security:

- Is access to servers restricted and monitored 24/7?
- Are thorough background checks done on all relevant personnel?
- Are you SAS 70 compliant? (Statement on Audit)
- Are you ISO 27001 compliant (Information Security Management Standards?)
- Is there systems redundancy in locations?

Data Protection:

- Is the data separate from other customers?
- Where is the data stored?
- Do you require encryption for all sign-ons?
- What are the authentication procedures?
- Can any third party access the data?
- Can you ensure that all my data will be erased at the end of service?

Data in Motion:

- How does data get transmitted from me to you?
- How is data transferred from one location to another?

Privacy

- Is critical data (i.e. credit card #, Social Security #, HIPPA) properly masked?
- Do only a limited number of authenticated and authorized people have access to critical data?
- Where is critical data stored?
- What are the conditions under which third parties, including government entities, might have access to the data?
- Can you guarantee that third party access to shared logs and resources won't reveal critical information about our organization?

Compliance

- Do you have disaster recovery and business continuation plans and can we review them?
- Where are your recovery data centers located?
- What level of service can you offer when under a disaster recovery conditions?
- Do you keep service + access logs? How long to you keep them?
- Will we be able to have access to them?
- Can we have dedicated access log and audit trail storage?
- Are all your data centers under local compliance?
- Does local compliance violate our agreement or any of our compliance requirements?
- Can you prove compliance for: PCI/SoX/HIPAA/ Basel II?

Legal

The Service Agreement and Contract is critical, here are some considerations to follow:

- Can the provider change things at will or with limited notice including hardware and other key technology?
- Does the provider have any performance guarantees?
- Who owns the IP?
- In the event of a security breach what is your recourse in the agreement?
- Can you own all your data including replicated and redundant copies?
- Is there a limitation of liability in the contract and is it fair to you?
- Is there a proper indemnification?
- Under what conditions can you terminate the contract, other than a full breach of security?

(information from Forrester Research)

Risk Transfer

There are a number of very broad and effective policies available as the final protection in the event of a data breach. In order to most effectively manage the placement and coverage your broker must be well versed in the details of cloud computing and the coverage interface. Policies, if properly negotiated can first party coverage for fines and penalties i.e. *M.G.L. 93-H*, as well as offer coverage for PDA's and memory sticks.

WGA's years of knowledge and deep expertise in the technology area can provide you with the skilled professional assistance in effectively managing a risk management plan, particularly when it comes to an emerging area like cloud computing. For more information, contact the Technology Practice Group or your WGA Account Executive at William Gallagher Associates or email us at info@WGains.com.

