Cloud risks

Striking a balance between savings and security

Prepared by:

Daimon Geopfert, Security and Privacy Leader, RSM US LLP
daimon.geopfert@rsmus.com, +1 312 634 3400

April 2013

An increasing number of companies are turning to the cloud to house technology systems, software and data. The cloud's allure comes from decreased costs, lower maintenance and diminished need for infrastructure, software and staff, all within a platform that appears safer than many internal solutions. While these are all benefits of moving operations to the cloud in an optimal situation, significant regulatory, security and privacy risks also exist.

With the surging popularity of the cloud and its professed cost savings, companies may initiate a transition without thoroughly evaluating, or while simply ignoring, risks.

However, there is no one-size-fits-all solution and the reality is that some organizational structures are not a fit for a cloud-based platform. Before making a jump to the cloud, companies must assess their needs as well as relevant regulatory and privacy demands to ensure their information is secure and unforeseen cost is avoided.

Unanticipated risk can derail a cloud implementation and more importantly, present potentially disastrous results. In most situations, the benefits of the cloud outweigh the risks, but organizations must be fully informed before making an investment.

Public vs. private

Organizations are presented with two options when moving to the cloud: public and private. Each offers a considerably different level of protection and support, with a financial commitment that also differs substantially. The private option carries more expense, but also more control around security and functionality. The increased expense of a private cloud increases the attractiveness of public cloud options, but public is not an appropriate solution for many organizations.

Public cloud

If an organization selects the public cloud option, its applications and data are stored on shared servers that hold similar information from many other organizations. With public cloud vendors hosting this information in the same environment, storage costs are minimized by dividing them between several different companies, making the solution less expensive.

The public cloud can be a favorable solution for simpler tasks such as email and basic file or document storage. However, it may not be the best choice for more complex operations, or for companies subject to regulatory requirements. With your data commingling with information from many other sources in the public cloud, regulatory violations are possible as data crosses state or international lines. Robust monitoring and if necessary, forensics, can be extremely challenging.

Private cloud

The private cloud is a more dedicated and controlled solution, as data is housed in a solitary setting within a vendor's, or your own, environment. The private cloud allows for more flexibility and control over data and access, as well as increased reporting and auditing capabilities. Large organizations with significant storage demands, or those subject to heavy compliance or legal regulations, are prime candidates for these "closed" environments.

However, as previously mentioned, the exclusivity that the private cloud offers comes with increased expense. Private environments are also often closely tied to their legacy environment and can inherit existing security concerns.

Security and privacy

Despite all of its positive attributes, the cloud is not always safer than on-premise alternatives. Security capabilities can differ greatly between vendors and cloud structure, and if not careful, organizations may simply be trading one type of risk for another. A cloud solution may be technically secure, but may not fully comply with legal and regulatory demands applicable to certain industries.

As cloud storage becomes more popular, it also becomes a more valuable target for hackers. The likelihood of a successful attack is low, but the impact could be enormous for both the public cloud, with its large amount of diverse information from many companies, and the private cloud, with its privileged information from a single firm. Vendor options can be overwhelming, but it is imperative to be careful in selecting a provider with security and privacy standards that meet your unique organizational and industry requirements.

Outsourcing risks

Outsourcing is a popular strategy to cut costs, but organizations should realize the potential impact of these solutions. The strategy removes a significant amount of local knowledge about your applications and their usage, and if a problem or abnormality occurs, it may not be recognized in a timely manner because of the new team's lack of familiarity. Without close monitoring, outsourcing often does not allow your company to view and manage applications as desired.

An outsourcing strategy does not eliminate the need for IT staff, as personnel are still necessary to maintain devices, such as user laptops, used to access data in the cloud. In addition, even with an outsourcing arrangement, many companies retain some IT infrastructure in house.

Additional costs

A cloud platform can significantly reduce IT costs for an organization, although the savings may not be as imminent as many expect. Cloud solutions often require revised business processes which carry an upfront financial and time expense, while special audits and regulatory reviews can disrupt normal operations. When evaluating a cloud platform, executives must ensure these risks are properly accounted for to avoid potential damage from lost productivity or sanctions.

Compliance concerns

Migrating to the cloud creates a host of compliance concerns, primarily related to regulatory requirements, such as Payment Card Industry Data Security Standards (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), Financial Industry Regulatory Authority (FINRA), and the Financial Information Security Management Act (FISMA/FedRAMP). These regulations are fluid and carry restrictions on how data is stored and the level of security that is placed on information and records. Organizations should confer with legal counsel and internal audit to determine which solutions comply with applicable guidelines, policies and regulatory requirements.

Conclusion

Motivated by expectations of lower costs through decreased personnel and infrastructure, many executives are pushing for the move to a cloud platform. It is an appealing model, but migrating to the cloud before evaluating security and privacy risks, regulatory impact and the potential for hidden costs can result in significant financial and reputational damages.

An organization considering a transition to the cloud must undergo an analysis to determine the true costs of an appropriate solution and whether the benefits outweigh the risks. A trusted advisor that understands your industry demands and the structure of your business can help assess available options, evaluate risks and compliance requirements, and determine whether the cloud is the right solution for your data.

+1 800 274 3978
www.rsmus.com

This publication represents the views of the author(s), and does not necessarily represent the views of RSM US LLP. This publication does not constitute professional advice. This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.