Analyst briefing:

Laying the groundwork for successful cloud deployment and management

By Tom Olzak
March 2013

Analyst briefing: Laying the groundwork for successful cloud deployment and management

Published by TechRepublic

March 2013

Disclaimer

The information contained herein has been obtained from sources believe to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

TechRepublic

1630 Lyndon Farm Court

Suite 200

Louisville, KY 40223

Online Customer Support:

http://techrepublic.custhelp.com/

Credits

Editor In Chief

Jason Hiner

Head Technology Editor

Bill Detwiler

Head Blogs Editor

Toni Bowers

Senior Editors

Mark Kaelin

Jody Gilbert

Selena Frye

Mary Weilage

Sonja Thompson

Teena Hammond

Graphic Designer

Kimberly Smith

Contents

Executive summary

When we talk about cloud services, we usually see challenges from one of two perspectives: security or services delivery. The problem is that these are inseparable parts of a cloud solution; one cannot take precedence over the other. Both business users and security analysts must learn to step back and shift perspective.

We should view cloud service management in two ways. First, it is a security issue. Moving data across our data center trust boundary presents special challenges. Second, we must see a cloud service as another link in our organization's supply chain. Interruption to services provided by our vendor cause business processes to fail, reduction to the bottom line, and other issues common to a supply chain failure. Both approaches feed a comprehensive risk management process to ensure continuous, safe business operation.

Before designing a cloud replacement or augmentation of your internal IT services, you must decide which deployment models and services you need and evaluate how well the provider offering matches your list of essential characteristics. In this briefing, we'll start by looking at each of the deployment models and service models. Then we'll consider the key characteristics of cloud service offerings, such as performance, reliability, and compliance.

The companion paper, "Analyst briefing: Conducting a cloud solution risk assessment," builds on this information and provides a roadmap for determining potential areas of vulnerability, mitigating risk, and implementing a comprehensive cloud management strategy.

Definitions

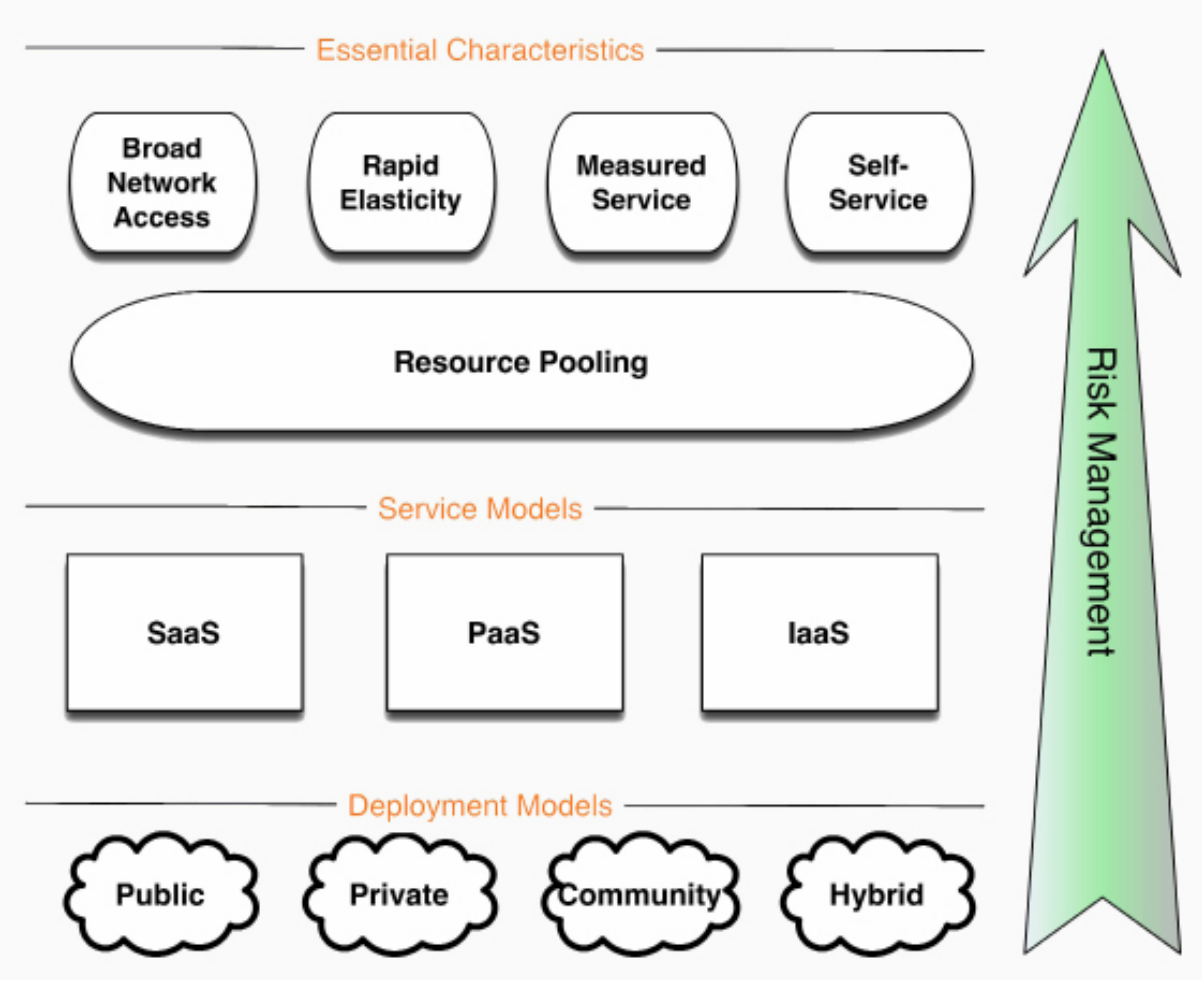
When Internet-based services first started to appear, and the moniker "cloud" was attached, many definitions of cloud emerged. It took several years, and much collaboration, to arrive at a meaningful description. For our purposes in this briefing, we'll use the generally accepted definition provided by the National Institute of Standards and Technology (NIST):

> "Cloud computing is 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" (Badger, Grance, Patt-Comer, & Voas, 2012).

Expanding the definition

This general definition is a good start, but it needs development before we can use it to assess, plan, implement, and manage a cloud implementation. **Figure A** depicts the various assessment targets when deciding whether—and how—to move a process to the cloud.

Figure A



Deployment models

An organization can choose one of four approaches to cloud deployment: public, private, community, or hybrid. No one approach is usually appropriate for all services placed in the cloud; each has unique advantages, disadvantages, and risks. Assessing which deployment model is right for your organization and the data/processes involved also requires understanding cloud characteristics and how they change between models.

Public

A public cloud consists of services hosted by a cloud services provider and open to the general public, an industry group, etc.

Private

A private cloud is either hosted and managed by a cloud service provider or the organization implementing the solution. In any case, the cloud infrastructure and services are used by a single organization.

Community

A community cloud expands the private model by adding additional organizations with similar or shared objectives (e.g., mission, security requirements, policy, or compliance).

Hybrid

Combining two or more of the previous models results in a hybrid deployment. Hybrid implementations provide opportunities for resource sharing and cost mitigation.

Service models

Within each deployment model, an organization can select the level of service that makes sense for the target process or data. As **Figure B** shows, each service—other than infrastructure-as-a-service (IaaS)—builds on a foundation created by a previous service.

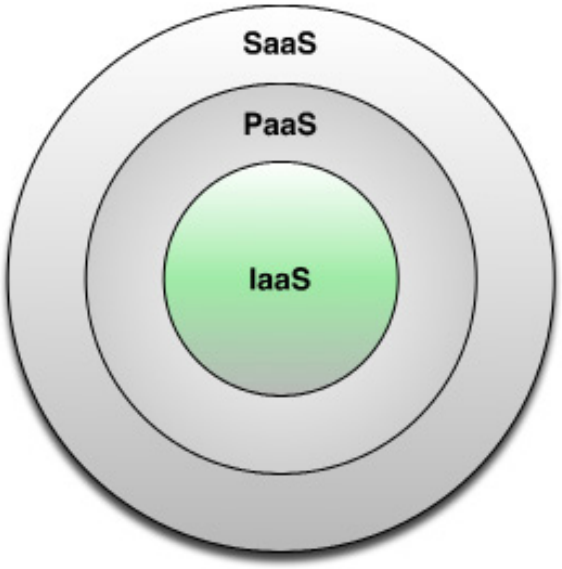


Figure B

IaaS

IaaS is a simple infrastructure offering. The IaaS service provider offers processing and storage hardware, with supporting network services, for use by your organization (the customer). The customer is responsible for all security and supply chain issues in operating systems and applications. IaaS provides significant flexibility, but it also requires the customer to retain much of the associated implementation and management costs.

PaaS

Platform-as-a-service (PaaS) extends IaaS by providing operating systems, database software, developer tools, and other components necessary to develop or install customer-managed business applications. When an organization chooses this service model, it is directly responsible only for security, implementation, and management of applications installed in the service-provider's platforms.

SaaS

Typically, the service provider owns and manages all components of software-as-a-service (SaaS) implementations. Users access the applications via Web browsers with few or no locally installed modules. With SaaS, the customer has oversight responsibility only for ensuring security and compliance.

Although organizations are not responsible for direct management of the services to which they subscribe, they still must provide adequate oversight to ensure their customers, their data, and their business processes are protected. We address these issues later in this paper.

Finally, many vendors have entered the cloud services market. It's often difficult to know whom to contact with questions about a specific service model. The Cloud Security Alliance (CSA) makes this a little easier by providing a Cloud Taxonomy chart in its Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.

Essential characteristics

When selecting the right implementation and service models for your organization, a solid understanding of potential cloud service offerings' characteristics is important, including

- Multi-tenancy
- Performance
- Reliability
- Cost/benefit
- Compliance
- Information Security

Multi-tenancy

In a multi-tenancy situation, multiple customer organizations share one or more resources. In situations where the service provider does not use virtualized servers, this can result in two or more organizations sharing an application server, database server, and other storage, network, and security resources. For many applications and data classifications, this is not enough separation.

The more likely scenario, however, is service provider provisioning of virtual servers. When properly managed (see Chapter 10 – Virtualization Security in *Enterprise Security: A Practitioner's Guide*, on the InfoSec Resources site), virtualized servers provide all the protection offered by discrete hardware. How well your data

and processes are protected largely depends on your continuous due diligence, regardless of who is directly responsible for resource management.

Computing performance

Not all business solutions are necessarily good fits for cloud computing. For example, email is a good example of an application with performance characteristics (both network and server) suitable for cloud hosting. However, a network resource-intensive application requires more cloud resources and better connectivity. In some cases, getting to the place where the user experience is satisfactory might eliminate any associated benefits. Badger et al. break down performance into the following key indicators (2012):

- **Latency** is a common measure of performance when evaluating user experience. It is the time between a user request and when the response appears on his or her screen.
- **Offline data synchronization** allows users to access documents and other important information when not online. This is often necessary when mobile users visit customer locations where guest Internet access isn't available.
- **Scalable programming** enables dynamic resource allocation. For example, an application that only occasionally needs extra processing power can scale out to use additional resources. When done in the cloud, your organization does not have to pay for the additional, unused resources sitting in your data center waiting for work. Rather, you pay for them when and if needed.
- **Data storage management** requires the same attention to data protection and availability as you apply to your in-house data center storage devices. Oversight of cloud-stored data requires initial assessment and continuous monitoring of five storage provisioning characteristics:
    1. How easy is it to expand storage as the business grows or storage needs change?
    2. What physical security controls protect the devices containing your data? (See Perform a physical security gap analysis.)
    3. How does the service provider restrict and monitor storage access, both physically and logically?
    4. Is storage shared? If so, how is your data segregated from other organizations?
    5. How is data deleted? Is it erased so recovery by unauthorized personnel is difficult or impossible? What is the service provider's process for disposing of storage media?

Reliability

Reliability is often touted as a measure of uptime. For example, a cloud service provider might claim five nines (99.999%) availability. The problem is that these numbers mean very little when your employees or customers can't access services. Further, what part of the provided services does this represent? In case of the inevitable failure, what is your maximum tolerable downtime (MTD) for each affected business process? Can the service provider recover before the MTD is reached? How can you be sure?

Reliability becomes the measure of how well your supply chain partner (the service provider) can provide promised services. This is the same challenge facing any manager responsible for supply chain management. While a supply chain consists of interconnected businesses, people, processes, and technology providing product and services for production or other business operations, supply chain management is (italics are mine):

> "…the *active* management of supply chain activities to maximize customer value and achieve a ***sustainable*** competitive advantage" (Handfield, 2011).

A cloud service provider plays a key role in your supply chain. Instead of providing raw materials and subassemblies, the service provider ensures that employees and customers can purchase and pay for product or services, review offerings, submit inquiries, etc. These and other business support capabilities are likely the reason your organization uses the cloud. In any case, ensuring continued availability requires active oversight on your part.

Oversight begins with a contract that stipulates your expectations and the provider's commitment. It continues with continuous monitoring of the objectives covered by your contract's service level agreement (SLA) and frequent (e.g., monthly) meetings to discuss shortfalls and other concerns. It is the service provider's responsibility to provide agreed-upon services, but it your responsibility to ensure that services meet management's expectations: achieving revenue, cost containment, and competitive objectives.

Cost/benefit

Two possible advantages of cloud computing are cost reduction and cost avoidance. Cost reduction can occur when the cost of provider management of services falls below the cost of maintaining them in-house. Cost avoidance is possible when, for example, an organization doesn't incur the full cost of new infrastructure and software when rolling out a new application or core business solution. As with any purchase, a cost/benefit analysis should precede any contract signing. When assessing potential benefits, a handful of risks might prevent moving a process to the cloud (Badger et al., 2012):

- **Business continuity** is a key concern, as we discussed in the section on reliability. If no service provider you assess meets MTDs, you should probably keep your processes in your own data center.
- **Service agreement evaluation** is another way of looking at your SLA negotiation. A cloud service provider must be flexible enough to adjust a boilerplate SLA to your organization's unique needs. Even if a single-instance MTD constraint is met, multiple instances can cause customer frustration and loss of employee productivity. These are just two ways to increase cost and reduce revenue: a bad way to get management's attention.
- **Portability of workloads** is a measure of how easily you can move business processes to the service provider's infrastructure. If the implementation cost is significantly greater than the overall operational savings over the life of a contract, management's cost reduction goals are missed. A true assessment of portability requires a deep look at infrastructure requirements, application interfaces, and other points of possible incompatibility.

- **Interoperability between cloud providers** is a necessary assessment for two reasons. First, many organizations use two or more service providers to implement related business processes. When input or output for a cloud-hosted business process is coming from or going to another cloud-hosted business process, the provider interfaces must work well together. It's also important to understand the willingness of each provider to maintain your organization's required interfaces, even if the majority of their other customers don't need them.

Second, the initial reliability and business stability of a provider might not last. In such cases, a move back to your data center or to another provider is necessary. Ensure that this move is as painless as possible with pre-defined methods negotiated with your providers. Further, understand the impact on your business if a provider ceases operation suddenly. What are your options and are they reasonable?

Compliance

Most organizations today fall under either government or industry governance related to how information is protected. Even if a provider's sales staff insists it meets all your compliance needs, verify anyway. In addition to initial verification, implement contract-assured processes to ensure continued compliance. Areas of concern include:

- **Visibility.** Under no circumstances should you do business with a cloud service provider that refuses complete visibility into how it ensures the confidentiality, integrity, and availability of your data. Accountability in the form of audit logs (logs you can access on demand) and third-party audits is necessary for adequate oversight. Finally, verify the provider's internal security processes, including access control, incident detection, and incident response.
- **Physical location.** Where a provider locates its data center directly affects your ability to protect both your data and the continued provisioning of business processes. If, for example, a provider chooses to cut costs and locate its data center in a country with lax laws, corrupt officials, or political unrest, you cannot assume the provider will continue to meet your compliance or availability expectations. Understand where your data and applications will actually reside and determine whether the risk associated with that location justifies the associated cost savings.
- **Forensics support.** When a security event occurs in your data center, incident response processes should help you arrive at the root cause and associated remediation steps. This requires visibility into logs and access to provider employees for interviews. When possible, ensure the provider uses a comprehensive security information and event management (SIEM) solution for continuous monitoring, detection, and incident resolution.

In addition to forensics analysis, when you receive a litigation hold notice, it is imperative that your provider has tools necessary to help you comply. Beyond the hold, the provider should also support e-discovery tools (theirs or yours) when the time comes to provide discovery documentation to opposing counsel.

Information security

We've already covered many characteristics of information security. This is always the case when we don't separate security from operational requirements. In every challenge faced during a cloud services assessment, security is an inherent consideration—and the provider should treat it as such. In this way, security isn't just slapped on during the contract review.

Again, visibility is critical. Demand to see the provider's security program (policies, standards, and guidelines). Review procedures affecting administrative, technical, and physical security. Where gaps exist, ensure correction before signing anything. Visibility and assessment begins with a risk assessment and ends with the completion of a remediation action plan.

Risk management

Risk management should govern all aspects of the evaluation, implementation, and management activities associated with integrating cloud services into your organization. Managing risk requires attention to the components of the risk formula shown in **Figure C**.

- **Probability of occurrence** breaks down into Threats x Vulnerabilities. Threats, and their agents (e.g., malware), exploit vulnerabilities (weaknesses) to reach target information resources.
- **Business impact** is the short- and long-term cost of a threat exploiting a vulnerability. It includes the cost of response, lost revenue, lost customer confidence, etc.
- **Controls** include administrative, technical, and physical safeguards that mitigate probability of occurrence and business impact. One primary control category includes safeguards to reduce or eliminate vulnerabilities. Another includes detection and response processes to mitigate business impact.

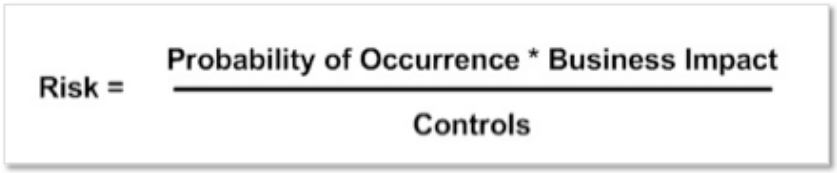


Figure C

Expanding the formula, managing risk is:

> "…the proper application of business risk mitigation tools and methods resulting in the implementation of security controls that, when operating properly—either alone or as part of a layered set of safeguards—mitigate business risk associated with an information system to a level acceptable to management. This must be done in a way that maintains the highest possible operational effectiveness of the personnel and processes using the systems protected by these controls" (Olzak, 2008, p. 3).

At this point, we've looked at all relevant considerations when assessing whether to move a process or its data to the cloud. The associated paper, "Analyst briefing: Conducting a cloud risk assessment," provides a high-level overview of how to perform a risk assessment for cloud or in-house information resources. The process is the same regardless of where you host your data data and processes. For a more detailed discussion of conducting a risk assessment, see Chapter 2 – Risk Management.

Key takeaways

- Managing the cloud is not much different from managing your internal network. The big difference is ensuring you have enough visibility into the provider's processes and technology to verify compliance with your expectations of confidentiality, integrity, and availability.
- Treat cloud services as part of your business supply chain. Ensure that each vendor is contractually bound to meet your business process continuity needs. Support this with clearly defined sanctions when vendors miss SLAs.
- Cloud services extend over three offerings: IaaS, PaaS, and SaaS. Starting with IaaS, each subsequent service builds on the previous. The point at which you take over is the security demarcation point—the point at which you take responsibility for policy compliance, availability, and incident response.
- Each cloud service offering possesses essential characteristics that define how the provider supports its customers and the customer experience. Assess each and negotiate characteristics compatible with your management's expectations and the business requirements associated with the processes sent to the cloud.
- Integrate your cloud service planning, implementation, and management into your existing risk management processes.

References

Badger, L., Grance, T., Patt-Comer, R., & Voas, J. (2012, May). Cloud Computing Synopsis and Recommendations (NIST SP 800-46). Retrieved February 10, 2013, from National Institute of Standards and Technology: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075

Handfield, R. (2011, January 11). What is Supply Chain Management? Retrieved February 12, 2013, from NC State University: http://scm.ncsu.edu/scm-articles/article/what-is-supply-chain-management

Olzak, T. (2008, February). A Practical Approach to Managing Informaltion System Risk. Retrieved November 9, 2011, from Tom Olzak on Security: http://adventuresinsecurity.com/Papers/Practical_Approach_IS_Risk_p.pdf

About the author

Tom Olzak is a security researcher for the InfoSec Institute and an IT professional with more than 30 years of experience. He has written three books, Just Enough Security, Microsoft Virtualization, and Enterprise Security: A Practitioner's Guide (to be published in Q1/2013). Before joining the private sector, he served 10 years in the United States Army Military Police, with four years as a military police investigator. He has an MBA and CISSP certification. He is also an online instructor for the University of Phoenix.

About TechRepublic Pro

TechRepublic Pro, TechRepublic's premium service, provides information that IT leaders need to solve today's toughest IT problems and make informed decisions. We distill complex tech topics into concise, yet comprehensive packages. Our ready-made policies, templates, and tools will save you valuable time and effort.

Visit us at www.techrepublic.com/pro.