

TECH INSIGHTS



weaver  IT advisory services

SUCCESSFUL CLOUD COMPUTING MIGRATIONS REQUIRE INFORMED DECISIONS

At any given time, how many individuals throughout the world are using Google's free Gmail service to send or receive email?

Gmail is an example of cloud computing at the software as a service (SaaS) level. Gmail users do not have to install any software, nor do they need to store sent or received messages for future reference. Gmail may also be accessed from any virtually any desktop computer, laptop or mobile device. The various conveniences Gmail offers individual users illustrate basic benefits associated with cloud computing.

At the most comprehensive level of cloud computing - infrastructure as a service (IaaS) - corporate customers may purchase virtually all of the IT functions they need from a cloud services provider (CSP). Such availability of IT capabilities at various service levels represents the fruition of a business model articulated decades ago.

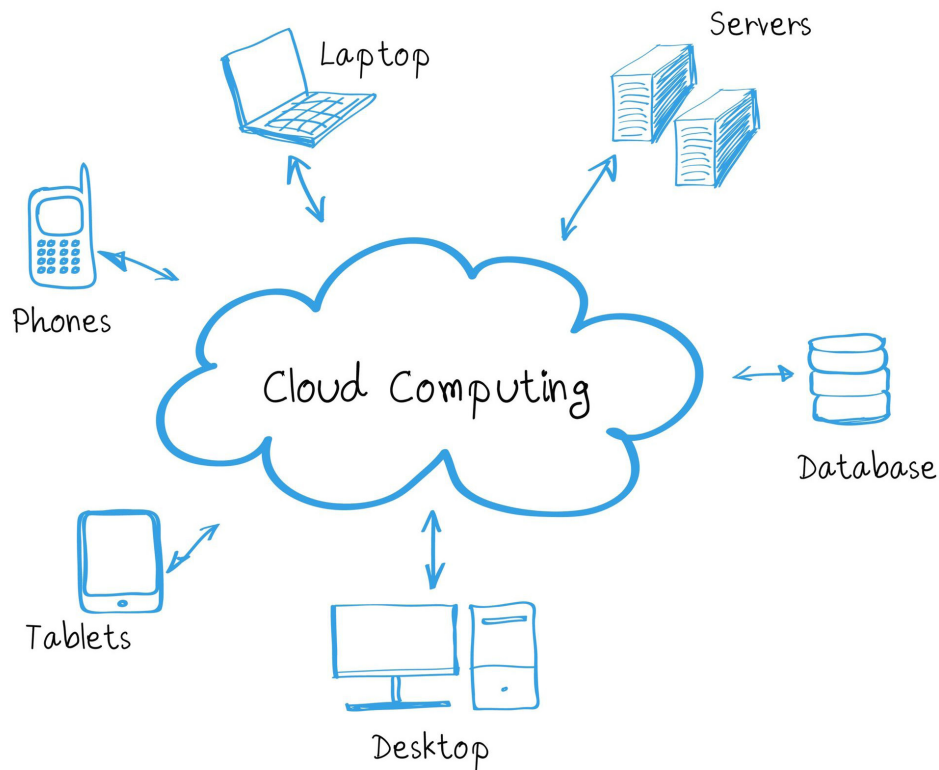
John McCarthy, a computer science professor at Stanford University, is widely credited with first proposing the cloud computing concept in the 1960s. At the time, McCarthy envisioned computing services being delivered and sold on as-needed basis, in much the same way that public utilities deliver various types of services to residential or commercial customers.

It took computing technology advances in general and extensive expansion of Internet transmission capacity in particular to make that concept reality. The 1999 introduction of Salesforce.com gave many corporations their initial experiences in capitalizing upon a robust SaaS application.

Within the past decade, an array of other software providers developed applications in SaaS format. Many of the largest technology companies in the United States, including Amazon, Google, IBM and Microsoft, introduced much more extensive cloud computing services, too.

That market growth and expansion reflects the growing interest prospective customers have in exploring the business advantages associated with migrating IT functions to a cloud computing environment.

WITH CLOUD COMPUTING,
PURCHASING AND IMPLEMENTING
ADDITIONAL IT SERVICES CAN BE
COMPLETED WITHIN A DAY.



The Potential Business Benefits of Cloud Computing

Cloud computing eliminates the fixed costs associated with maintaining vast IT capabilities in-house. Cloud computing may also reduce the amount of time leaders and managers must commit to some of the more mundane IT concerns, enabling an organization to apply greater financial resources and organizational focus toward more strategic activities.

Organizations face varying needs for IT capabilities and capacity over time. The ability to purchase IT services “on demand” from a CSP eliminates having to either maintain greater IT capacity than what is normally needed, or face difficulties at peak requirement times.

Expanding or upgrading in-house IT capabilities typically requires detailed planning and considerable time. With cloud computing, purchasing and implementing additional IT services can be completed within a day. That flexibility allows organizations to more quickly respond to changing business conditions, including growth opportunities.

When organizations consider cloud computing’s potential benefits, they also need to be aware of levels of service generally offered, and how much they wish to outsource to a CSP.

The Three Basic Levels of Cloud Computing

Cloud computing comes in three general levels: Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS).

SaaS is the least extensive and most common forms of cloud computing, with the software developer providing hosting of a software application. Customers may access a SaaS application via a standard Internet browser.

Application enhancements and upgrades are performed by the CSP. Users may have some software configuration options. In addition to Salesforce.com, other well known applications offered in SaaS format include SAP and IBM Lotus Live. As with other levels of cloud computing service, SaaS offerings are typically sold on subscription or “pay as you go” pricing plans.

PaaS enables companies to deploy their own or acquired applications within a cloud computing infrastructure, rather than being solely dependent on SaaS vendors’ offerings. Microsoft’s Windows Azure platform is an example of PaaS, as is Google’s App Engine platform.

IaaS offers provision processing, networking components, data storage and other functions. It represents the most extensive level of cloud computing. IaaS enables customers to have not only extensive software customization options, but also full virtual server capabilities and immense data storage capacity. Well known IaaS providers include Amazon Cloud Services and Rackspace.

Cloud computing offers substantial potential benefits, and various CSPs provide those varying levels of computing services. Organizations considering a migration to a CSP, though, need to evaluate the remaining potential IT vulnerabilities.

Cloud Computing Presents Risk Considerations

Organizations face IT risks related to data integrity, data privacy, security, system availability, system reliability, and data retention. While contracting with a CSP essentially outsources computing functions, organizations must still consider how those IT risks are addressed by the CSP. They must consider data ownership as a concern, too.

With an in-house application, automated controls may prevent the system from processing an incomplete entry. Once an entry is accepted, system processing may automatically transfer that data to other databases requiring that information. A potential cloud customer needs to understand how such data processing integrity needs are met within a CSP's systems.

Nonpublic information needs to remain private. The CSP needs to sufficiently segregate data so that it cannot be viewed by unauthorized employees or other cloud computing customers. Key access, data encryption, data masking and related privacy concerns must be addressed.

Vulnerability concerns with cloud computing encompass both physical and logical security considerations. What controls exist to restrict physical access to a CSP's facilities and the equipment and data residing inside?

The immense volume of data handled by CSPs makes them appealing targets to hackers. The CSP must maintain effective firewalls, address known vulnerabilities, and implement other logical security measures to deter and quickly detect any attempts at unauthorized access or denial of service. CSPs must also implement measures to address the retirement of older equipment including data destruction policies.

Needs for CSP service fluctuate among customers. While the "on demand" aspect holds considerable appeal, the CSP has must have sufficient capacity to ensure that services are available during regular use periods, as well as during times when customers may be facing peak service requirements.

CSPs need to perform regular maintenance or equipment upgrades to maintain reliability. Sufficient backup systems and processes are needed to provide continuous service during such times. The CSP must also have a disaster recovery plan in place to minimize any service disruptions if a natural disaster or other adverse event occurs.

While CSPs have capacity to hold vast amounts of customer data, a potential customer needs to determine how long information is retained and if it can be readily accessed.

The speed at which service may be initiated with a CSP gives cloud computing considerable appeal. However, the ease with which cloud services can be initiated also has downside in that

resources may be deployed rapidly without addressing specific risks. For example, a cloud customer needs to retain ownership of that data and control over how or when that data may be securely moved or shared. A prospective cloud customer should also evaluate the financial stability of a CSP to mitigate the risk of losing data if that provider were to abruptly cease business operations.

Specific Compliance and Regulatory Concerns

In addition to general IT-related vulnerabilities, potential CSP customers need to consider the specific legal and regulatory concerns they face, and how migrating IT operations to a cloud computing environment could affect compliance with those requirements.

Thanks to technological advances, information may be rapidly transmitted across state and national borders. To determine whether or not contracting with a CSP raises various legal and jurisdictional concerns, though, a potential customer needs to identify the actual physical location where data is held and CSP services are performed.

Legal provisions also require that corporations retain and make various types of data accessible for electronic discovery requests that arise during litigation efforts. A cloud customer must ensure that the services provided by the CSP meet such requirements.

Additional compliance measures that prospective CSP customers may need to consider include, but are not limited to:

- **Sarbanes-Oxley Act** requirements as they relate to public corporations and their internal controls over financial reporting, including work performed by service organizations.
- **Health Insurance Portability and Accountability Act (HIPAA)** requirements regarding the privacy and security of protected health information (PHI).
- **Gramm-Leach-Bliley Act (GLBA)** requirements facing financial institutions for safeguarding customer information.
- **Payment Card Industry Data Security Standards (PCI DSS)** requirements for mitigating the risk of credit card fraud.
- **Federal Trade Commission (FTC) Red Flags Rule** requirements for credit issuers to assess and mitigate risks for identity theft.

A potential customer needs to be aware of those or any other applicable compliance measures and determine how meeting those requirements could be affected by migrating IT functions to a CSP. Details of how those compliance requirements would be met then need to be discussed with a CSP and documented in a service level agreement (SLA).



CSPs need to perform regular maintenance or equipment upgrades to maintain reliability. Sufficient backup systems and processes are needed to provide continuous service during such times.

In addition to considering compliance requirements, a potential customer also needs to evaluate what would be the most relevant assurance report to request from a CSP.

Attaining Relevant Third-Party Assurance

A cloud computing customer needs an independent auditor's assurance that the CSP has designed and implemented effective measures to identify and mitigate relevant risks.

A SAS 70 report was often viewed as a de facto standard of assurance for all third-party service providers, even though it was not it may not have been the most appropriate means for gaining assurance regarding a CSP's controls.

SAS 70's popularity grew after the Public Company Accounting Oversight Board (PCAOB) guided in 2004 that SAS 70 could be used for reporting on the effectiveness of a service provider's internal controls. The PCAOB guidance, though, only applied to Sarbanes-Oxley compliance and financial reporting tasks performed by a service provider.

SAS 70 was retired in 2011 and replaced by the Statement of Standards for Attestation Engagements No. 16 (SSAE 16). In conjunction with that transition, the American Institute of Certified Public Accountants (AICPA) introduced its three Service Organization Controls (SOC) reports: SOC 1, SOC 2, and SOC 3. A SOC 1 engagement is based on SSAE 16 and may be best suited to organizations that appropriately relied upon SAS 70 for Sarbanes-Oxley compliance.

The SOC 2 and SOC 3 reports are based on the AICPA's Trust Services Principles of Security, Availability, Processing Integrity, Confidentiality, and Privacy.

For customers more focused on attaining assurance for compliance and operational concerns as they relate to a CSP, the SOC 2 or SOC 3 should serve as more effective reports.

A SOC 2 report addresses at least one of the five Trust Services Principles. The report includes a description of the CSP's system, a CPA's opinion on the fairness of the presentation of that description, as well as a description of tests performed by the service auditors. The report also includes the results of those tests. With its emphasis on the Trust Services Principles, the SOC 2 report enables a customer to attain assurance for more relevant IT issues.

While also based on the AICPA's Trust Services Principles, the SOC 3 report is more of a general use report and only includes the auditor's report on whether the system achieved the Trust Services criteria. The report may be issued on one or more of the Trust Services Principles. A CSP with a SOC 3 report is allowed to post the SOC 3 Report: SysTrust for Service Organizations seal on its website.

Determining which report is most appropriate depends on the scope and specific types of services provided by the CSP, as well as the compliance requirements facing the cloud customer.

The Information Systems and Audit Control Association (ISACA) and the European Network and Information Security Agency (ENISA) offer additional direction for IT-related audits that best address a potential CSP customer's needs.

Cloud Computing Effectiveness Hinges on Informed Decisions

Cloud computing offers immense potential advantages, including lower IT costs and greater business flexibility. Fully benefiting from cloud computing, though, requires understanding how service is provided, what an organization's needs are, the potential vulnerabilities associated with such a migration, and how various compliance and assurance needs that must be met. With such preparation, organizations are more likely to attain the benefits of cloud computing without being subjected to acute, unforeseen difficulties.

CONTACT US

BRIAN THOMAS, CISA, CISSP
Partner, IT Advisory Services

Brian.Thomas@weaverllp.com
713.800.1050

Weaver has offices throughout Texas.
More at weaverllp.com