

Cloud computing as a concept is having a huge impact on business and IT strategy . Gartner identifies cloud computing as the #1 strategic technology that organizations need to plan for in 2010, up from #3 in 2009.¹ The appeal, of course, is expected cost savings; increased speed to market; and massive elasticity, scalability, and flexibility . Cloud computing, nevertheless, has many challenges ... beginning with finding an agreement on what defines cloud computing and how we talk about cloud services, the architecture, and delivery of cloud offerings . One point on which there is agreement, however, is that the top concern about cloud within enterprises is security, according to a recent survey by IDC .² This paper offers a point of view on cloud services, its definition, and an outline of the opportunities cloud services bring to the enterprise, while clearly detailing how to best manage the related technical and business security risks .

Cloud services: securing a business advantage for your enterprise

The usage of cloud services is seeing explosive growth, offering compelling, scalable, and elastic solutions in addition to benefits such as on demand, pay-per-use, and even resilience over existing Internet protocols . Because of this, vendors of all types are marketing a broad spectrum of products and solutions as “cloud services,” even relabeling their existing products with cloud terms . As a result, many organizations, and often individual business units, are jumping headlong into cloud computing, or—at the other extreme—trying to avoid it however possible . Because there is so much hype and confusion around the word and the concept, HP approaches cloud services as an opportunity to re-examine both business and IT strategies, with a focus more on desired outcomes and specific deliverables—for example, new compute capacities that adjust with business needs and offer countless ways to deliver .

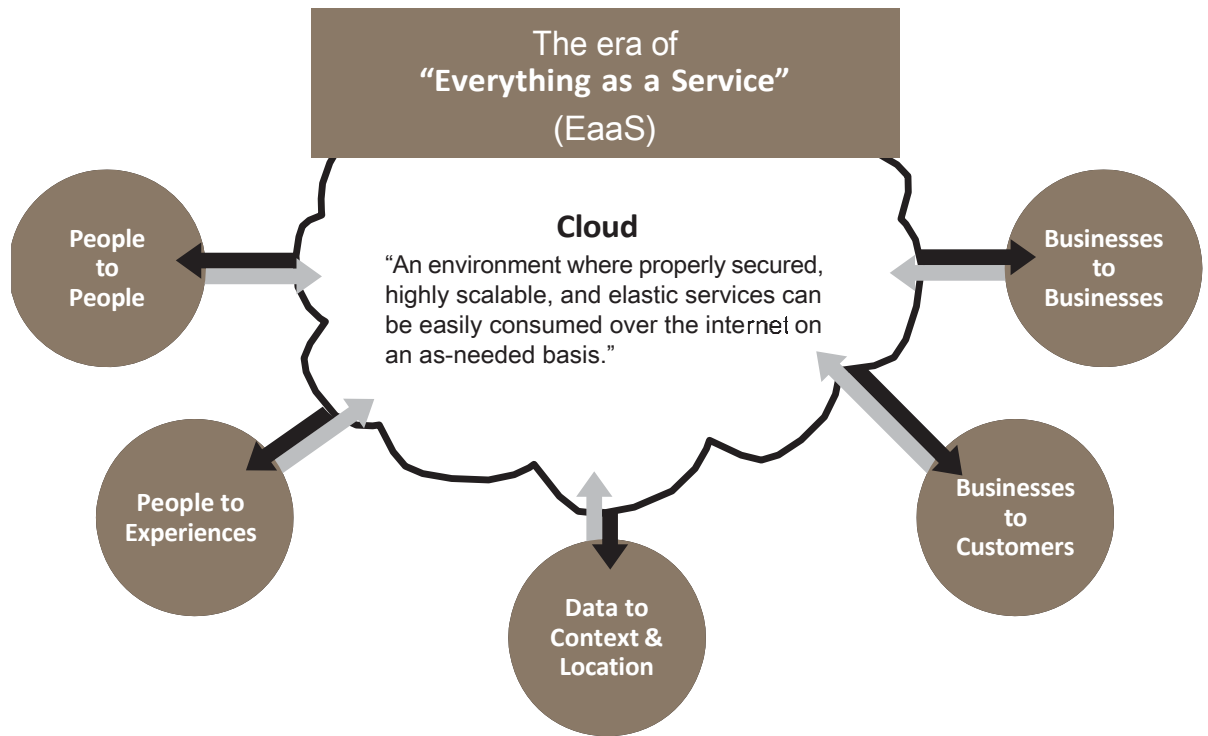
This new model for delivering solutions has many positive aspects, but it may not be suitable for many scenarios, especially as they relate to large enterprises and public service organizations . There are inherent issues of data integrity, compliance, service levels, architecture, and—most significantly—security . However, the blanket term “security,” like cloud computing itself, in many respects, is too broad . The requirement then is to clearly identify the specific components of an organization’s security posture, using an agreed-upon taxonomy . There are industry efforts under way, with key groups strongly supported by HP: The Cloud Security Alliance (CSA) published a set of guidelines for cloud security and created a set of use cases to help refine an understanding of the requirements; and The Jericho Group, part of the Open Group, offered a model for secure cloud collaboration before joining forces with the CSA to advance the effort . Using standards and industry approaches is a good baseline but requires a level of mapping to and from specific enterprises’ taxonomies and business requirements .

To secure the most benefit, HP recommends a classic risk management strategy alongside the integration of an evolved distributed computing and service oriented approach to enterprise architecture . It is not always wise, or possible, to utilize current cloud

¹ <http://www.gartner.com/it/page.jsp?id=1210613>

² IDC, Cloud Computing 2010, An IDC Update, #TB20090929, September 2009.

Figure 1: Cloud—Everything as a Service



computing models for critical enterprise applications or anything that incorporates critical business data . HP offers a comprehensive portfolio of products, services, and partners, along with 30-plus years in distributed systems security, to help clients defend, protect, and validate their long-term IT strategies for cloud computing . HP has defined a taxonomy that incorporates focus areas of: **Data Privacy and Protection; Identity Management; Governance, Risk and Compliance; and Infrastructure Security and Readiness** to collaborate with clients and identify their critical concerns and responses, and secure their business processes and IT .

This viewpoint paper details the above approach and discusses key examples of how to employ best practices and tools to gain critical business advantages and outcomes from cloud services .

Introduction

The cloud offers a vast selection of services that yield new kinds of business value for any organization wishing to take advantage of Internet technologies . HP sees cloud computing as a logical evolution of IT strategies including grid, utility, on-demand, and distributed computing .

Cloud services aligns closely with the HP strategy and vision for our partners and clients of "Everything as a Service" (EaaS) . Many definitions exist for cloud, and most align with HP's and extend the previous memes of Web 2.0 and distributed computing . In a nutshell, it is a means by which highly scalable, technology-enabled services can be easily consumed over the Internet on an as-needed basis . This definition, like most others, doesn't accommodate any requirement for proper or even minimal security, assuming perhaps that security is inherent . This is far from the reality . Although many cloud service providers incorporate

Figure 2. Commonly cited benefits of cloud services

	Commonly cited benefits	Rationale
1	Simplify and optimize the IT environment	Less to own and operate
2	Avoid capital expenses	Consumption-based pricing
3	Faster ROI—less to build	No building assumes faster delivery & ROI
4	Better agility to meet business needs	Composing external services allows for quicker reaction to business needs
5	Low-cost disaster recovery	Assumed cloud services already have some level of disaster recovery

Figure 3: Commonly cited concerns of cloud services

	Commonly cited concerns	Rationale
1	Service level agreements	Poor or nonexistent service level agreements on performance, availability, and support
2	Data security, legal, and regulatory controls	Immature controls, processes, and certifications in place to manage risk
3	Vendor lock in	Lack of interoperability between cloud services (Platform as a Service [PaaS], Infrastructure as a Service [IaaS])
4	IT management issues	Services, data, and vendors still need to be managed; lack of adequate tools to manage and extract data
5	Market flux/immaturity	Concerns around vendor viability, service quality, and support

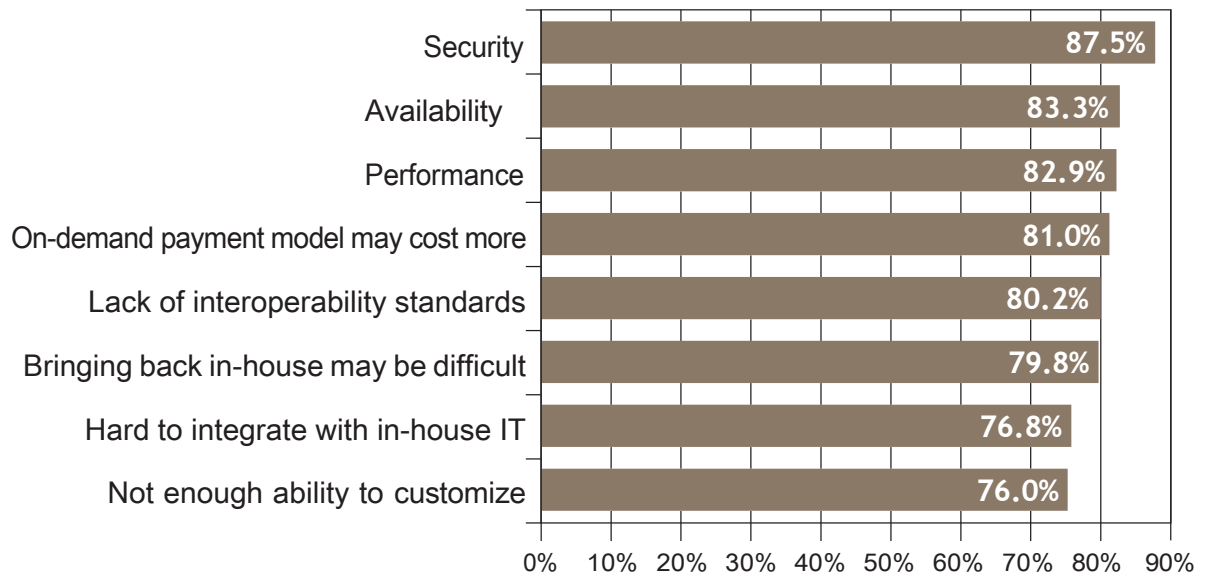
security into their approaches, they rarely align their security solutions with traditional enterprise client security approaches for reasons of scale, flexibility, and cost. Fundamentally, many clients and providers of cloud services achieve these obvious benefits at the expense of security. HP believes that secure cloud computing will allow you to more rapidly evolve business strategy. By refining your security requirements, there is the opportunity to identify cloud services to enable business outcomes while maintaining your security posture.

Regardless of the ultimate definition or terms used to describe this extended approach to business, it is more important to focus on your organizational needs in relation to the potential benefits, weighed against potential risks, in a classic approach to business risk management.

Figure 2 shows the commonly cited benefits of cloud services. The real business opportunity, as a result of such flexibility, is allowing organizations to rapidly adopt technology choices through an optimal method to mix-and-match cost structures for minimizing capital expenditure (CapEx) and funding new projects through operational expenditure (OpEx).

As a result, many are approaching cloud computing solutions with board or executive support and a resultant nonchalance, intentional or not. Business units and end users are buying IT services without understanding the fundamentals of maintaining enterprise functions. The most common cited concerns to HP around cloud computing are described in Figure 3.

Figure 4: IDC 2009 Enterprise Panel Survey—Rate the challenges/issues of the 'cloud'/on-demand model



(Scale: 1 = Not at all concerned; 5 = Very concerned)

Source: IDC, Cloud Computing 2010, An IDC Update, #TB20090929, September 2009.

Security is high on the list. This aligns closely with multiple analyst reports, including IDC's 2009 survey of 263 respondents to their IDC 2009 Enterprise Panel shown in Figure 4.

Assuming that cloud solutions are less secure than those housed in large IT data centers is a common reaction. While sometimes true, it is certainly not always so. By preparing to use cloud services with a risk-based approach in mind, concerns can be addressed through process, planning, risk analysis, and governance. Cloud solutions increase requirements associated with policy enforcement, while at the same time offering opportunities to decrease requirements around managing physical infrastructure. Considering that many especially smaller enterprises cannot staff a full-time security team, cloud or outsourced solutions provide compelling options in terms of cost and capability.

Understanding the risk-based requirements will position enterprises for business enablement with the appropriate level of security. IT departments have a critical role to play in this by advocating a measured approach, as well as offering an expedient framework for the business to securely use cloud computing solutions.

To succeed, however, requires a much better understanding of what the market means when it talks about cloud services. The amorphous properties that are used to describe cloud computing do not include security, or truly break cloud down into something that is manageable.

Figure 5: Cloud services and industry examples

Types of Cloud Services	Description	Industry examples
Cloud-driven processes	• Architecture of participation, crowd sourcing, perpetual beta, network effects	• Ratings, Review, Comments • Open Source Software, Mark
Software as a Service (SaaS)	• Consumer-focused web sites—rich Internet applications • Multi-tenant business-focused web applications • Collaboration, email, office productivity, CRM	• Flickr.com, Snapfish.com • Myspace.com, Zillow.com • Google Apps • Right Now • Salesforce • Cisco WebEx
Platform as a Service (PaaS)	• APIs for specific service or capability access or integration • Data or capability web services • Application composed (mash-up) via UI-centric configuration and scripting • Configuration and scripting platform	• PayPal, Amazon FPS, DevPay • Yahoo APIs (Search, Flickr) • Google APIs (Payment, AdSense) • JackBe • BEA Aqualogic • Rollbase • Zoho App Creator • Caspio • SharePoint
Infrastructure as a Service (IaaS)	• Hosted application development environment • Application infrastructure capabilities • Database, data stores • Message queues • Virtual servers, logical disks, compute capacity enabled by API-based provisioning	• Google App Engine, BigTable • Microsoft Azure—SQL DS • Amazon Simple DB, S3, SQS • Force.com • Amazon EC2 • FlexiScale • Elastra • RightScale • Mosso • GoGrid

The cloud ecosystem

Most industry experts tend to consider cloud computing as a set of layered service-based solutions. The most common approach to defining cloud computing is a

three layer model of services—Infrastructure, Platform, and Software, each riding atop the lower layer. The cloud-driven processes connect business process workflow across enterprise processes and information. Figure 5 presents examples of each of these layers.

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/268032132133006022>