

Cloud computing issues and impacts

[VIEW NOW ►](#)

Contents

4 Overview: clouds are inevitable

All signs point to the rapid adoption of cloud computing as a fundamental shift in the delivery model of information technology (IT) – but abundant challenges will make it a difficult adoption curve.

11 Drill-down discussions

Nine detailed reports explore the specific benefits, risks, accelerants and inhibitors associated with the following critical aspects of cloud computing adoption:

- Pricing and business models 12
- Vendor management and strategic sourcing 18
- Availability and interoperability . . . 22
- Security and privacy 26
- Standards and risk management . . 30
- Government 34
- Accounting 38
- Cross-border taxation of CSP arrangements 42
- Regulatory compliance 46

50 Outlook

Higher-level business processes as a service will evolve rapidly atop cloud-based IT services, leading to the increasing rise of incredibly agile virtual organizations.

52 Glossary of terms

A list of new words and phrases that cloud-based IT models have placed into the business vernacular – including a widely adopted definition of cloud computing and its characteristics, service and deployment models.

54 Source notes

“By concentrating technology in the cloud, making it available as a service and freeing organizations to focus on business strategies – that’s how the IT industry will once again not only transform business, but business models.”

Pat Hyek

Global Technology Industry Leader

Cloud computing issues and impacts

Estimates of 2010 worldwide revenue from cloud computing services range from a low of about \$12 billion to a high of slightly more than \$68 billion – reflecting different views and means of evaluating this fast-growing technology phenomenon.^{1,2} Where the market researchers all agree, however, is that cloud computing is no fad. Cloud computing is a fundamental shift in IT that will alter the technology industry power structure, improve business agility for all industries and increase everyone’s access to computing, storage and communications power. As one prominent research house put it in the title of a report containing cloud predictions for 2011: *“Welcome to the New Mainstream.”*³

Despite the certainty expressed in these predictions, the transition to cloud computing from in-house IT infrastructure and traditional outsourcing is really just beginning. By the end of 2011, public and private cloud services will generate 15% of worldwide IT spending.⁴ There is a long, hard road of difficult transitions and adoption decisions still ahead.

Right now, however, is when cloud service providers (CSPs) need to position themselves, their offerings and their future development strategies for the rapid changes to come. Likewise, business users of cloud services require immediate insight into the benefits and risks of cloud computing – along with how to exploit the former, while avoiding the latter – as they adopt this “new mainstream”

IT approach. Finally, both technology and other businesses need to understand how cloud computing is changing consumers’ habits and expectations.

Cloud computing issues and impacts combines the insights of Ernst & Young’s own leading thinkers with analysis of secondary market research and other sources to synthesize our view of the current state of cloud computing, where it is going in the foreseeable future and the holistic way you should think about it. Through this series of topical drill-down discussions, we offer our insight and hope to stimulate productive dialogue within and across your organizations about how to make the most of the transformative force of the cloud.

Note: unless otherwise indicated, all quotations are from practitioners at member firms of the global Ernst & Young organization.

Overview: clouds are inevitable

“Clouds can free companies from the drudgery of building and maintaining IT infrastructure so that they can focus on value-creating differentiation to ride atop that infrastructure.”

Kevin Price
Global Technology Industry
Advisory Services Leader

Current situation

The IT services now known as cloud computing have been around for decades, but they never grew beyond a small fraction of total industry revenue. Now, however, their time has come: over the past few years, a dizzying array of hardware and software available as services over the internet has emerged. Consumers and businesses have embraced a multitude of cloud services, from mature sales force management services to email and photo editing to the latest smartphone applications and the entire social networking phenomenon. Further, researchers project an imminent inflection point in the adoption of cloud services by organizations both large and small.

In fact, research firm International Data Corporation (IDC) calls cloud computing the foundation for the technology industry's next 20 years of growth, saying, “it is nothing less than the complete transformation of the industry's core offering and business models.”¹ According to IDC, public clouds (delivered to multiple customers via the internet) and private clouds (built by or delivered to a single organization via private network) will account for 15% of IT spending in 2011 and grow at a compound annual rate of about 26% for the next four years. This is roughly five times the growth rate of the technology industry as a whole. In addition, 80% of all new software offerings in 2011 will be available as cloud services (regardless of whether they are also available via traditional on-premise business models).

Technology advances, business agility drive cloud adoption readiness

Cloud services are finally taking off because technology advances, particularly ubiquitous high-speed internet connectivity and the ever-decreasing cost of storage, have finally enabled service providers to meet buyers' needs for simplicity, cost and flexibility. For consumers, the recent proliferation of smart mobile devices that are actually handheld wireless computers has accelerated the development of cloud services that provide application functionality to those devices. This is an example of why consumers have been such rapid adopters of the cloud: cloud computing has the potential to instantly deliver simple, easy-to-use, sophisticated and high-powered computer applications and information that consumers could not otherwise access.

“European companies and governments view cloud computing as a way to stimulate business activity and create opportunities for future growth.”

Rebecca Norris

Europe, Middle East, India and Africa (EMEIA)
Technology Industry Leader

For business organizations, the core elements of CSP business models have always been attractive: pay-as-you-use instead of install-and-own, and inherently greater flexibility in IT. Cloud computing services generally shift major up-front capital expense from the buyer of IT to the provider of IT services – a strong incentive in a world that continues to struggle with economic uncertainty and more restricted access to capital. Of note, this shift enables organizations to further manage their investment risk by rapidly implementing and trialing new solutions before making long-term commitments.

Even more alluring for businesses, however, is the promise that cloud computing will increase their business agility in at least two dimensions. “First, clouds can free companies from the drudgery of building and maintaining IT infrastructure so that they can focus on value-creating differentiation to ride atop that infrastructure,” explains Kevin Price, Global Technology Industry Advisory Services Leader. “Second, clouds provide flexibility in the form of highly elastic scalability, enabling organizations to rapidly increase or decrease their IT infrastructure costs as fast as their business needs change,” he adds. That flexibility dimension is the primary way in which cloud services differ from traditional IT services, and why some experts refer to cloud computing as “the next generation of outsourcing.”

These factors combine to lower IT barriers (and risk) to business change, including barriers to entry for start-up businesses, whether entrepreneurial or inside an established organization. The same factors also enable small- and medium-sized businesses (SMBs) to take advantage of sophisticated applications and a breadth of functionality that previously could be afforded primarily to large enterprises only, and can do so at much lower cost. As a result of these factors, SMBs appear to be migrating to the cloud more rapidly than larger companies, and start-ups are virtually all cloud users. An example already in progress is the mobile applications market: it is relatively new, is cloud-enabled, includes a plethora of small companies that sell directly to consumers via app stores and is projected to grow to \$32 billion by 2015.² As cloud adoption becomes widespread, its characteristic of enhancing business agility is likely to lead to an increasing pace of change for all industries worldwide.

Adding fuel to the interest in cloud computing is that cloud services advance “green” agendas: they allow fuller utilization of shared infrastructure capacity, thus consuming less power and lowering the carbon footprints of their users versus alternative IT approaches.

CSP considerations

CSPs are in the enviable position of being early movers in a movement that is rapidly becoming mainstream. Yet the challenges they face are unenviable, starting with the difficulty of translating theoretically advantageous business models into concrete services and pricing programs in a young, still-developing market.

Setting prices, for example, may seem simple but becomes complex fast because cloud monthly service fees may be compared with the amortized total cost of ownership (for their entire useful life) of those elements of a customer’s IT infrastructure that don’t enhance competitive differentiation. Yet the complete economic picture does not reside in cost alone. Variables such as rapid access to new technology and the ability of cloud customers to focus their internal resources on what differentiates them should also be factored into the economic equation.

Standards, particularly for interoperability among clouds and between clouds and in-house infrastructure, are another area of uncertainty. Real standards leadership – not just empty promises – might be a winning strategy for CSPs, but it is a difficult choice given the trade-off with vendor lock-in.

CSPs also need to decide whether to build their infrastructure to enable compliance with different rules from region to region, or to provide a homogenous global cloud. A related issue is how much transparency into their infrastructure they should allow customers. Both of these issues have cost implications that are likely to affect pricing.

However, given the core premise of the CSP model – solving difficult IT challenges once and spreading the solution among multiple buyers – CSPs can transform each challenge into a new opportunity. For example, “compliant clouds” have recently emerged, offering compliance with specific regulations to companies that need it. Many other so-called specialized clouds are likely to emerge rapidly as the cloud model matures.

Cloud computing

services are available across the entire computing spectrum

Clouds offer full range of computing services

Cloud computing services are available across the entire computing spectrum. The US National Institute of Standards and Technology (NIST) has published a definition of cloud computing that has been adopted and referred to internationally and which we have included in its entirety (see Glossary, page 52). While the US NIST definition includes three primary service models, the market has evolved so that you can buy as a service just about any slice of the computing “stack” within the three, which are as follows:

- ▶ **Infrastructure as a service (IaaS):**
raw computing power, storage and network bandwidth
- ▶ **Platform as a service (PaaS):**
databases, development tools and other components required to support the delivery of custom applications
- ▶ **Software as a service (SaaS):**
applications both general, such as word processing, email and spreadsheet; and specialized, such as customer relationship management (CRM) and enterprise resource management (ERM)

In addition, we believe a fourth service model is evolving, albeit more slowly at present than the primary three. Business process as a service combines multiple components of each of the primary three to deliver an entire business process.

Today, services such as payroll and billing already can be outsourced using traditional methods. Looking ahead, we expect higher-value business process services to evolve, differentiated from traditional business process outsourcing because they will ride atop multiple underlying cloud services and an organization's internal staff typically will work the process. These new services will be based on the ability of business experts in different domains to optimize a process and deliver it via cloud-based IT services. Ultimately, future organizations may create innovative offerings by combining such optimized services (see Outlook, page 50).

Transforming inhibitors into accelerants

An unusual, perhaps unique characteristic of cloud services is their ability to transform today's challenges into tomorrow's adoption drivers. In surveying dozens of sources, we observed multiple examples of this apparent paradox. For example, security is cited more than any other factor as a reason why IT managers are hesitant to adopt cloud services. Yet Forrester Research projects that within five years, cloud security will become one of the primary drivers for adopting cloud computing.³ The reason for a shift of security from obstacle to driver is that CSPs are expected to invest far more in the development of their security infrastructure and expertise than any typical enterprise.

Likewise, regulatory compliance in multiple jurisdictions, especially regarding privacy and data location, is another challenge to cloud adoption. In response, some predict the creation of specialized “compliant clouds” that will offer certified compliance with specific regulations for different industries, including a guarantee to store and manage data within the borders of a given nation, as appropriate.⁴

The generalized lesson we take away from this analysis is that the most difficult challenges facing in-house IT organizations are ripe opportunities for CSPs. CSPs that solve the problem once, using leading practices, can then offer their solution as a service to all who need it.



Cloud adoption accelerants

Many factors are causing momentum to build for mainstream adoption of cloud computing, some of which have been mentioned already. Importantly, there are examples of relatively mature and successful cloud offerings for businesses, such as sales force management services, to learn from. The cloud accelerants that support business agility and flexibility – such as elasticity, pay-as-you-go and market barrier reduction – are among the most important on the following list:

- ▶ **Elasticity** – the ability to scale IT infrastructure requirements both up and down rapidly, on a pay-per-use basis, is extremely attractive to large and small organizations alike (see page 23).
- ▶ **Pay-as-you-go versus install-and-own** – the shift in up-front capital requirements from the user to the service provider is equally attractive – again, to large and small organizations alike (see page 12).
- ▶ **Cost savings** – a report by the Brookings Institution finds government agencies can save 25% to 50% of their IT costs and increase their business agility by migrating IT infrastructure to cloud services (see page 34).
- ▶ **Market barrier reduction** – cloud computing services reduce IT barriers to market entry, enabling far more start-ups to emerge with much lower infrastructure costs than were necessary pre-cloud. This increases innovation in and of itself and also spurs larger organizations to innovate more rapidly.
- ▶ **Infrastructure utilization** – better network efficiency results in lower power consumption and smaller carbon footprints. This comes from virtualizing hardware and software resources and providing them as a service to multiple users simultaneously. Additionally, large CSPs can increase network efficiency through global load balancing. If a CSP's customers are spread across the globe, peak usage times will be spread over the course of each day as workers from different geographies hit their peaks at different times.
- ▶ **Public investment** – governments worldwide are investing to create economic regions of cloud technology development (e.g., China, Japan), are supporting cloud-related standards development (e.g., EU, US) or are migrating their own IT infrastructures to cloud services in an effort to lead by example (e.g., US, UK, Japan) (see page 34).
- ▶ **Market research** – research points to ongoing rapid adoption of both public and private cloud services, which tends to become a self-fulfilling prophecy.
- ▶ **Security** – delivering “security as a service” eliminates one of in-house IT's greatest non-value-adding challenges (see page 26).
- ▶ **Standardization efforts** – standards will reduce or eliminate risk from many current barriers to cloud adoption (see page 30).
- ▶ **Cloud brokers** – emerging cloud services brokers simplify an organization's transition to the cloud by helping to overcome specific security, privacy and compliance issues and helping achieve interoperability across multiple public clouds, private clouds and in-house IT infrastructure.
- ▶ **Risk of missing out** – organizations that do not adopt cloud computing along with their competitors risk missing out on expected benefits such as the flexibility and agility afforded by on-demand services and access to the latest versions of technologies. This is because CSPs typically perform more timely upgrades than most private organizations.

“Asian nations are investing in cloud centers of economic development and are adopting cloud services for their own use. They are very focused on the cloud opportunity.”

Joe Tsang
Asia-Pacific
Technology Industry Leader

Business user considerations

Organizations are attracted to the opportunities cloud computing offers to lower their costs and free their best technology managers to focus on creating strategic differentiation. It's likely they would be even more excited if not for all the change cloud computing requires.

The clearest change required for the transition from in-house IT infrastructure to cloud computing is the shift to managing service quality and availability through contracts and relationships, rather than through specifications and direct technology implementation. But this implies an even larger corporate culture challenge: because different skills are required, existing IT staff will likely need to be retrained or replaced. Organizations face a conundrum: if they attempt the cloud transition with existing staff they will likely meet internal resistance, but new staff would lack knowledge of company processes.

Another challenge organizations face is the need to better understand the dependencies among their own various systems, which have built up over years or even decades, in order to manage processes that combine their own infrastructure with a CSP's.

Organizations also must consider how transitioning to an external cloud affects enterprise risk, especially with regard to data security, privacy, uptime and availability as well as regulatory and legal compliance. But cloud computing also is likely to have an influence on more traditional ERM considerations, such as legal liabilities and brand protection.

For all these reasons, leading organizations are exploring cloud services by building internal private clouds for applications involving sensitive processes and data, while simultaneously investigating public clouds using non-sensitive processes and data. However, as cloud service maturity levels evolve rapidly over the next few years, it's important that organizations consistently revisit strategic sourcing decisions. The potential for migrating specific applications to the public cloud will change over time.



“The industry already is providing hardware, software and services to customers. Where customers spend their money will move from traditional vendors to cloud service providers, and any net incremental revenue to the industry will come from increased value creation.”

Paul Chabot
Global Technology Industry
Advisory – Process Improvement (PI)

Cloud adoption inhibitors

While cloud services are simpler to use and less costly than many in-house alternatives, they add complexity to the businesses of established companies entering the cloud computing market, whether as service providers or users. The delivery of cloud services is leading to new, multilayered revenue streams with increasingly complex and uncertain security, privacy, tax and related compliance and control consequences for cloud computing users and providers alike.

However, none of these challenges are impenetrable obstacles, and many can be turned into accelerants by CSPs that address them with leading practices, as described earlier. Still, these are the reasons why cloud computing adoption will be a long, difficult curve, especially for large organizations and governments. Among the inhibitors are:

- **Corporate culture shock** – particularly the belief that “we can do it better ourselves.” Separating themselves from the underlying technical implementation and focusing on differentiating value-add for their organization is a big shift for IT managers. No less daunting is the shift

from being an internal provider of services to a manager of external service providers, described next.

- **Loss of control** – instead of controlling the IT environment directly, through the implementation of technical specifications that they define, cloud users manage their IT infrastructure through their relationship with their CSPs and through service level agreements (SLAs). This requires skills that IT organizations typically do not possess today, so they will need to reinvent themselves to make this shift (see page 18).
- **Information security** – today, opinion is divided about whether protecting your corporate data in the cloud, both to be certain it is there when you need it and to safeguard it from unauthorized access by others, is more difficult than doing so on your own. Either way, ongoing analysis of how internal applications exchange data with cloud-based services and continued enhancement to security software and controls are called for (see page 26).
- **Privacy concerns** – cloud computing can complicate how you safeguard the personally identifiable information of your customers, business partners and

A brief history of cloud

Although it feels like cloud computing has arrived all of a sudden, the reality is that it has gone through decades of slow evolution.

In the late 1950s, when computers were massive and costly, hardware time-sharing (a label later co-opted by the resort vacation industry) emerged. As the concept expanded to include more than sharing a processor, it became known as “utility computing” and then “grid computing” in the 1980s and early 1990s. These were hazy visions that remained dreams, because even their proponents knew they lacked an efficient delivery mechanism.

But the ubiquitous broadband connectivity proliferated by the internet solved that service delivery problem. Applications service providers appeared in the late 1990s to much fanfare and excitement, but most burst with the rest of the internet bubble. As broadband deployment became widespread in the early 2000s, however, start-ups touting a range of services delivered via the internet cloud, from storage backup to enterprise applications, began to emerge. Established companies recognized their familiar vision and jumped into the cloud computing business with gusto.

Those decades of evolving experience are the reason that so many different cloud computing services have appeared so rapidly now that the conditions are finally right.

employees, both to meet your organization's own legal and ethical requirements and to comply with the privacy regulations of all the jurisdictions in which you do business – or through which your cloud passes (see page 26).

- **Regulatory compliance** – cloud services are delivered by “virtualizing” hardware and software that could theoretically be located anywhere in the world. Thus, cloud computing raises new questions about whose rules must be followed (see page 46).
- **Lack of standards** – many standards are required to simplify interoperability among cloud providers and between enterprise systems and cloud services, but few exist. The lack of standards also may pose obstacles to recovering data, whether for the purpose of legal discovery or for migrating from one CSP to another (see page 30).

Continuously monitoring cloud-enabled change

Nine drill-down discussions beginning on page 11 explore the accelerants and inhibitors described above in more depth. However, each accelerant and inhibitor will apply differently to individual organizations,

and their effects will change over time. It's important to consider them in the context of your own organization, its culture, its IT infrastructure and its opportunities and risks.

It is also important to consider them now. Our own global information security survey found that 45% of its 1,598 respondents from 56 countries have either already deployed or are evaluating cloud computing.⁵ An industry research firm predicts that as a result of cloud computing by 2012, 20% of business organizations will no longer have any IT assets of their own.⁶ That's just one year from now.

Technology companies should be evaluating their cloud strategies and determining the best opportunities to position themselves for the next decade of growth, which will be built on the foundation of cloud computing. And business users should be exploring opportunities to deploy cloud services pilot projects, or should be learning from their existing pilots and preparing to incorporate lessons from them into future deployments.

The cloud magnification effect

While cloud computing is viewed sometimes as a radical enough shift by itself, when cloud platforms interact with other technology trends the effects can be magnified.

- **Maintaining freedom of information:** when internet communications were shut down during recent unrest in Egypt, a team of international companies combined cloud services and social networking to connect in-country mobile phone networks to deliver text messages internationally via Twitter, in just a couple of days.⁷
- **Broadening frontiers of transformation:** while cloud computing has been with us in some form for many years, the continuously falling costs of computing, data transmission and storage are constantly broadening the opportunity for cloud services to transform businesses and business models, suggesting that cloud effects, ultimately, will be ubiquitous.
- **Enabling social networking:** although the widespread effects of social networking on businesses, governments and lifestyles is the province of its own report, it's important to note that those effects are significant, worldwide, and that the entire social networking phenomenon is enabled by cloud computing. Many believe the eventual impact of social networking on businesses and the related improvement in productivity will be profound.
- **Accelerating technology transitions:** one big difference between the successful introduction of tablet computers in 2010 from earlier failed attempts is that cloud-based services are available today to do the background computation, storage and other “heavy lifting” that make tablet computers useful tools.

Consumer considerations

Given that they generally have no data centers of their own, individual consumers have been embracing cloud computing since long before the cloud label even appeared. Search engines may have been the first cloud-based services that consumers adopted en masse; social networks are a more recent example. And as recently as September 2008, the Pew Internet & American Life Project reported that 69% of US residents who are online use web-based email, store data or use other software applications over the internet.⁸

Since then, the smart mobility “megatrend” has accelerated the use of cloud applications by consumers. Smart mobility is the evolution of mobile handsets into handheld wirelessly networked computers – devices capable of interacting with cloud-based software to provide a plethora of information services to their users. Not surprisingly, much of the software sold through smartphone app stores actually consists of just the display and user interface components of sophisticated applications that mostly run in cloud data centers.

The combination of cloud-based applications and smartphones has given consumers unprecedented access to information from wherever they are. This is transforming consumer expectations – heightening expectations for instant access to information and increasing the desire for personalized information. At the same time, social media have created a forum in which consumers are voicing their expectations – and businesses have begun to listen. In these ways, the “consumerization” of technology is having a profound impact throughout the global economy – especially by making inevitable the transition of businesses to the cloud, as more and more cloud consumers come to expect similar experiences at work.

Consumers have shown, time and again, that they will rapidly adopt cloud services with the right value proposition. Given the recent rise of personal privacy concerns, those value propositions may need to include privacy guarantees going forward.

Pricing and business models | Vendor management and strategic sourcing | Availability and interoperability | Security and privacy
Standards and risk management | Government | Accounting | Cross-border taxation of CSP arrangements | Regulatory compliance



Drill-down discussions

Getting granular on critical aspects of cloud computing

As mainstream adoption of cloud services begins in earnest, there is a multitude of factors that CSPs and cloud users must carefully consider. Our drill-downs explore the specific benefits, risks, accelerants and inhibitors associated with critical aspects of cloud computing adoption.

12 Pricing and business models

Multiple challenges – from encouraging customer behavior that smooths consumption highs and lows to overcoming obstacles to optimal asset utilization – complicate cloud business models and the pricing programs that manifest them.

18 Vendor management and strategic sourcing

Many organizations are still developing the skills necessary to achieve and maintain desired levels of service through vendor contracts and relationships; plus, cloud services demand new thinking about strategic sourcing opportunities.

22 Availability and interoperability

Achieving the efficiencies and scalability promised by cloud services – in the absence of proven standards – requires diligent investigation of both your own systems and your provider's.

26 Security and privacy

Relinquishing control over corporate data and the additional exposure of transmitting information over the internet are important concerns that must be thoroughly addressed.

30 Standards and risk management

Cloud computing can cause important changes in the ways businesses approach risk management, compared with in-house IT; industry standards help mitigate risks, but cloud standards are still immature.

34 Government

Despite impediments specific to their nature, governments are pursuing cloud computing with gusto, both to reap the same benefits as private organizations and to create leading cloud development and service centers within their borders as a source of economic development.

38 Accounting

Cloud services typically combine many elements of traditional IT infrastructure, resulting in significant revenue recognition and timing challenges for providers.

42 Cross-border taxation of CSP arrangements

CSPs face complex tax issues because cloud computing is often borderless, but tax regulations are not.

46 Regulatory compliance

Cloud services pose compliance questions for their users – which can translate into opportunity for their providers.

Drill-down discussion

Pricing and business models

“Cloud providers have to show customers a cost advantage that is not only better than what they’re paying today, but also is large enough to offset the cost of changing to a new approach.”

Joe Lackner
Advisory – PI

Current situation

At first look, cloud computing business models appear deceptively simple. Instead of buying and installing all their IT infrastructure and applications themselves, cloud customers buy access to the infrastructure and applications they need as they need them. Instead of paying for it all up front, including more capacity than they may need right away, cloud customers pay only for what they use – and only as they use it. Customers generally pay either a flat-rate subscription fee per user, or pay-as-you-go usage fees for precisely defined service levels.

Look deeper, however, and nuances emerge, multiply and become complex.

First, cloud service fees are just very different from how most companies think about the cost to build their own IT infrastructure. So at any price, CSPs face a daunting task in articulating to potential customers how they create tangible economic value compared with customers’ existing models. No less difficult is the task of determining the right price points. That analysis must encompass the full range of costs necessary to sustain a CSP’s service over the long term (including upgrades, maintenance, capacity planning and incorporating innovative

new technology, to name a few), while at the same time considering less tangible values, such as eliminating the uncertainty of building your own IT infrastructure when IT is not your core competency. In addition, customers’ consumption patterns and optimal network utilization must be factored into pricing considerations. Similar to many utility company “peak hour” and “volume” pricing programs, doing so enables cloud service pricing programs to offer incentives to customers to make their best efforts to use the cloud service efficiently, and establishes appropriate value for a CSP’s ability to provide elastic scalability that matches customers’ changing needs.

Pricing and business models | Vendor management and strategic sourcing | Availability and interoperability | Security and privacy
Standards and risk management | Government | Accounting | Cross-border taxation of CSP arrangements | Regulatory compliance

The “simple” cloud business model may be equally daunting. Business models for SaaS, for example, tend to become more complex as one moves from simple, standardized applications such as word processing to more complex applications such as enterprise resource planning (ERP). In addition, compliance requirements imposed by many governments that restrict where data and processing can physically occur tend to complicate all cloud business models by creating obstacles to optimal infrastructure utilization.

This is a new market, and few providers or customers have extensive experience with cloud computing business models and pricing, so further changes likely lie ahead.

Cloud pricing considerations

The main pricing complications for CSPs come from articulating all of the value captured in the price, determining what value customers will ascribe to buying the service instead of building the infrastructure themselves and pricing the peaks and valleys of consumption. If, for example, the top e-commerce sites all migrate to the cloud, how will their CSPs charge for the tremendous seasonal activity spikes that accompany retail sales? How will they encourage greater utilization during low usage times? (See Figure 1, below.)

Figure 1: Important cloud pricing and business model considerations

Issue	Implication
Maximizing asset utilization	Pricing programs must encourage customer behavior that helps smooth consumption peaks and valleys
Granularly detailed services pricing	Enables customers to optimize service cost via their software design, but could increase vendor lock-in
Capital expenditure	Corporate preference to use traditional return on investment (ROI) measures in making capital expenditure decisions could apply downward pressure to cloud pricing
SaaS customization	Because it requires non-standard, negotiated pricing, customization reduces the potential economic benefit of cloud models
Functionality “menu”	If providers make all functions available from a configuration menu, the possibility of differentiation via IT is diminished or eliminated
Funding innovation relevant to customer subsets	Given shared infrastructure, the economic model is unclear for innovation that benefits only a few customers; clearinghouses or application exchanges may evolve to fill the need
National regulation, particularly of data location, security and privacy	Creates obstacles to optimal asset utilization of cloud infrastructure

Source: Ernst & Young analysis.

Questions to consider

Cloud business user

- Does my CSP charge a premium for consumption that exceeds agreed-upon levels?
- Should I risk increasing CSP “lock-in” by optimizing my software design to take advantage of my infrastructure or platform CSP’s particular pricing approach?
- How much customization does my application require, and how does my CSP charge for it?
- Are there any relatively obscure software functions that my organization nonetheless depends on?

Cloud service provider

- What is the economically justifiable price point for my service, and how will it change over time?
- How can I structure a pricing program that helps to smooth out consumption of my infrastructure?
- What is the best model for deploying new functionality to my customers? Is an “open source” model an option?
- Does it make sense to expose discrete elements of functionality for separate purchase by customers?
- How often should we re-evaluate our pricing model to grow revenue?

“Who owns the responsibility for the upkeep of custom code in a SaaS model? To me, that’s the big dimension that makes it different than infrastructure or platform as a service.”

Joe Lackner
Advisory – PI

Similar challenges in traditional markets have been addressed via special pricing programs, most notably by power utilities and mobile network operators. Power utilities and their commercial customers typically agree to a threshold below which the customer pays a standard rate; for example, up to 20% above the customer’s average usage. However, if the customer needs 30% more power during a given usage peak, they may pay a significantly higher rate for the 10 extra percentage points. “Cloud pricing likely will end up in a similar place, because the cloud is all about capacity planning and infrastructure balancing, so there has to be some incentive for the customer to manage that supply and demand,” explains Joe Lackner, Advisory – PI.

Pricing effect on interoperability; capitalization versus expensing

IaaS and PaaS providers have broken up their service into many itemized offers; they charge separately for processor time, database reads and writes, storage capacity (charged differently for the disk on the server versus a remote disk), bandwidth consumed and more. One outcome of this detailed pricing strategy is that customers can choose to design their software in ways that lower the cost of cloud services.¹ For example, one leading IaaS provider prices processor time cheaply relative to the other service components, while a major rival prices processor time as a scarce commodity.

In this example, because of code differences, a customer that optimizes its software code for low cost using either CSP’s cloud would have a hard time migrating that software to the other CSP’s cloud – thus complicating the issue of interoperability among clouds.

Capitalization versus expensing is an issue that could put downward pressure on any CSP’s pricing model. Many corporations develop annual IT capital expenditure budgets based upon traditional IT infrastructure costs, and generally consider ROI metrics in making capital expenditure decisions. Depending on the pricing model of the cloud service, cloud vendors and users will need to understand how to make similar evaluations, as the nature of cloud service arrangements may not fit with traditional ROI measures. Even if a company determines that a cloud vendor’s offering is the better choice from an ROI perspective, organizations may find that they don’t have room in their current operating budgets to adopt the vendor’s offer, due to the fact that the CSP’s offering is a service and not a capital asset.

Furthermore, capital assets are generally depreciated or amortized over the useful lives of the underlying assets, while cloud services are generally expensed over the term of the arrangement. The classification of these expenses may also impact the decision to purchase cloud services, particularly for companies that measure themselves based upon traditional operating measures, such as earnings before interest, taxes, depreciation and amortization (EBITDA). “That, in turn, puts pressure on pricing models and, overall, on whether the value proposition works for one company at one specific time,” Joe says.

Further complications for SaaS

Pricing for SaaS may seem simpler, at first, because it is generally offered as a flat subscription fee – an amount per user, per month, with all the infrastructure details submerged into the application functionality. SaaS pricing also must consider how to smooth out the peaks and valleys of consumption, but for SaaS CSPs that is only the first of many complications.

Pricing and business models | Vendor management and strategic sourcing | Availability and interoperability | Security and privacy
Standards and risk management | Government | Accounting | Cross-border taxation of CSP arrangements | Regulatory compliance

SaaS CSPs must also determine how to charge for the value of configuration and customization and include separate charges for service integration with in-house customer applications – as well as ongoing incremental innovation and upgrades. Therefore, the complexity challenge for SaaS CSPs is to describe their per-user fee in a way that shows how it offsets the capital expenditure costs of setting up new infrastructure (up front and as a company grows) and includes the notion of having the latest functionality without the pain of major software upgrades and licensing costs.

Certain leading SaaS CSPs have good models for deploying new functionality, but they are based on limited experience with a small, pay-as-you-go set of applications and limited points of integration between the CSP and the customer's IT environment, which doesn't lend itself to being customized. If the SaaS market grows as robustly as most observers expect, such "limits" will be vastly expanded, and SaaS CSPs will have far more complex scenarios to deal with than currently is the case.

Because cloud computing is still in its early stages, many of these pricing issues blur together with business model issues.

Cloud business model considerations

In the case of relatively simple, standard productivity applications such as email, word processing and spreadsheets, SaaS business models are also relatively simple and standard. Advertising supports "free" versions; business customers that want additional support, storage, reliability or functionality pay monthly subscription fees per user. Slightly more complex applications typically charge an up-front fee for setup and a monthly service fee with a variable component based on a relevant usage parameter, such as web page views, ad impressions or email deliveries.

ERP and other enterprise-level applications, however, can be very complex and are sometimes customized to the needs of an individual organization; even consumption patterns are likely to be unique from one company to the next. Pay-as-you-use subscription models for ERP software delivered as a service might have to support custom configuration and development as well as ongoing support for the customized configuration.





Agreements involving such applications are likely to be individually negotiated and to include a definition of expected consumption patterns as well as special fees for differing from the expected pattern. The more customized the application becomes, the more unique pricing and contracting will be; pricing for complex SaaS services, therefore, may turn out to be not all that different from current outsourcing negotiations today.

Is a functionality "menu" a possibility?

Offering a "menu" of discrete functions around a core set of functionality is another possibility for how SaaS business models could evolve. Modern software typically provides far more functionality than any individual customer ever uses but offers no way to opt out of specific functions – you just ignore those you don't use. Many customers have their "favorites" among the lesser-used functions, and some customers are truly dependent on certain of them. Allowing a customer to pay only for functions they use might create value and simplicity for the buyer – but increase management complexity for the provider.

Extended to its logical conclusion, the functionality menu concept gets to the heart of whether an organization believes its IT systems can be a source of differentiation. If all potential options are available to be configured from a menu, as opposed to custom-developed, it suggests that IT isn't a differentiating factor. "What companies will want to do will bump up against the limit of what's pure configuration versus customization. So, while we will have more commonality over time, I don't think we'll get to a point where the application environment can become a box to check," says Joe.

Funding ongoing innovation

Funding for the development of the lesser-used functions described above may also become an issue. Innovation that serves the needs of the many will always find funding because it has an inherent model for ROI. But what of innovation that serves the needs of the few? Every major software release usually includes a handful of new functions that many users ignore but that are very important to a small number of customers. It remains unclear how CSPs will fund those types of functions.

Pricing and business models | Vendor management and strategic sourcing | Availability and interoperability | Security and privacy
Standards and risk management | Government | Accounting | Cross-border taxation of CSP arrangements | Regulatory compliance

Among the concepts that have emerged in response to this concern is the idea of clearinghouses or exchanges for innovation. Linux open source software development provides a potential model for the clearinghouse concept. In the Linux model, developers in the open source community offer new ideas and software code to a neutral party (in the case of Linux, a “benevolent oligarchy” of individuals) that decides what to include in future releases of the Linux software. An exchange would more likely look like the “app stores” that have evolved in recent years, initially around smartphones. Exchanges would enable “the few” who might be interested in an obscure function to find it and buy it, thus providing the economic incentive a developer needs to create the function.

Business model challenges

National borders represent a challenge to cloud business models because they can be a force in opposition to good asset utilization, which is one of the key drivers of economies for CSPs. Many nations impose rules on privacy, data location, management location or all of the above. Without such rules, CSPs would build services on top of infrastructure that resides in whatever country can offer the lowest total cost of

ownership, allowing for issues such as transfer pricing and tax liability. That way, a CSP could maximize the asset utilization of its infrastructure. However, when strictures are applied, the CSP must turn each stricture into a higher price point for the customer.

Besides pure cost issues, there is a balancing challenge for asset utilization. If an infrastructure provider has data centers in the US, Canada, India and China, for example, but every customer in China must run off the Chinese data centers, the CSP cannot easily balance its asset usage and will likely lose efficiency.

To accommodate these challenges, CSPs are likely to develop pricing models with multiple tiers for different service levels that relate to customers' tolerance for certain risks – most notably the compliance, privacy and security issues described above. For example, factoring strict compliance with the laws of multiple national jurisdictions into a service would cause that service to be priced higher than the same service without any compliance strictures. Likewise, “platinum” level security would be priced higher than “bronze.”

Ernst & Young observations

To properly value cloud services in the context of their own costs, customer organizations should start by determining the total cost of ownership (for their estimated useful life) of those elements of their IT infrastructure that are non-differentiating.

The complete economic picture does not reside in cost alone. Variables such as rapid access to new technology and the ability to focus internal resources on what differentiates your organization should also be factored into the economic equation.

Pricing and business model considerations for cloud services are particularly complex at this point because the market is so new that most offers are not yet well-defined. This will work itself out rapidly, as the market is evolving fast.





Drill-down discussion

Vendor management and strategic sourcing

An overwhelming number – estimated to exceed 60% of enterprises both large and small – will evaluate and pilot some type of cloud-enabled outsourcing offerings within the next 18 months.¹

Current situation

Cloud computing comes with a unique set of vendor management challenges and new criteria to evaluate when considering strategic sourcing models and analyses.

Vendor management in the cloud

The new vendor management challenges stem from the loss of control and lack of transparency into infrastructure details that often come with moving to cloud services from in-house or traditional outsourcing models. Before, companies could design systems to meet – or, if outsourcing, specify – precise requirements for security, data integrity, system availability, privacy and other factors. Moving to the cloud means buying from CSPs that do not always provide a transparent view into the inner workings of their infrastructure. While the exact nature of the issues vary depending on the type of cloud service (e.g., application, platform, infrastructure), the overarching principle is the same: instead of specifying technical requirements, business users typically must manage vendors to meet service levels using SLAs.

Strategic sourcing in the cloud

Cloud computing also changes strategic sourcing equations in at least two dimensions. First, complications around data security, privacy and compliance in the cloud will influence the types of applications and business processes that are candidates for cloud deployment, as opposed to traditional outsourcing. Second, system interdependence will similarly have an influence. Complex interdependencies may make it very difficult to extract a given application from the rest of the enterprise infrastructure; also, the solutions that address many business processes are likely to involve both cloud-sourced and in-house elements that must interact. The effort required to achieve that interaction across the enterprise-cloud boundary will affect the strategic sourcing decision. In addition, different cloud opportunities will mature at different rates; for example, security issues might be resolved before compliance issues involving privacy or tax. Therefore, as the market evolves, strategic sourcing opportunities determined to be unfeasible today may become feasible tomorrow – but which ones become feasible, and precisely when, will depend on how the market evolves.

Accelerants

Emergence of cloud service “brokers”

Cloud service aggregators, or brokers, are already beginning to emerge to help organizations overcome their initial lack of experience in managing CSPs, especially for situations in which multiple CSPs may be required.² Service aggregators sit between the cloud and the client to actually package all of the services based on the needs of the organization. They then manage the governance and the service levels for the organization. Venture capital (VC) funding is accelerating this trend. VCs wish to participate in the cloud opportunity but generally try to avoid capital-intensive businesses that require massive data centers, such as have been constructed by Amazon, Google, Microsoft and others for the provision of cloud services. Service aggregators are a more natural fit for VC funding.

Standardized SLAs, personnel shift and time are needed

Though it may sound like a cliché, time is likely to be among the most important accelerants of cloud adoption for issues such as vendor management and strategic sourcing. Over time, the experiences of early adopters will lead to standardized SLAs that help define critical components of the relationship between organizations and their CSPs, as well as how to manage those relationships. Such standardized documents can be put to use by organizations that don't have their own direct experience. It will also take time for organizations to shift their personnel from technical experts capable of directly managing an IT infrastructure to people skilled at managing complex multifaceted relationships with vendors. Finally, time plays a role in strategic sourcing, because different cloud services are maturing at different rates, and what organizations consider strategic or tactical also tends to change over time. However, these changes will not take a long time, because mainstream cloud adoption appears to be happening rapidly.

Questions to consider

Cloud business user

- ▶ Do we have the necessary skills and discipline to manage multiple vendor relationships to meet critical business requirements?
- ▶ Am I aware of all of the cloud services being used by my organization in all of its distributed global operations?
- ▶ Are all of our internal system dependencies well understood, or will we need to sort out those dependencies before making use of cloud services?
- ▶ Should I consider the use of cloud service “brokers” to accelerate either adoption or pilot projects?

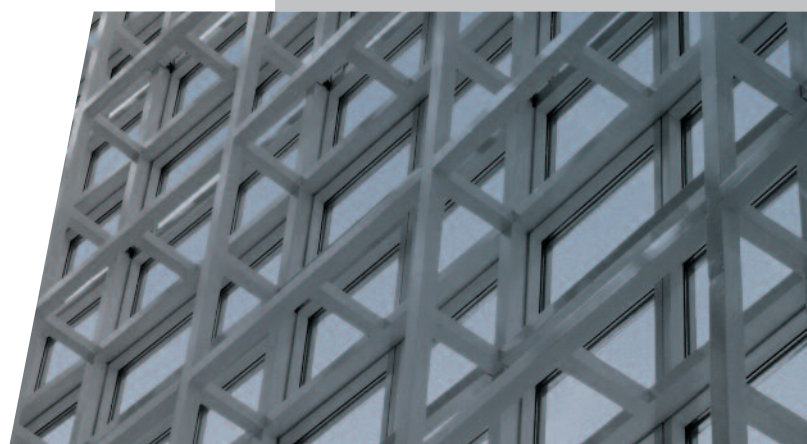
Cloud service provider

- ▶ Given customers' inexperience with SLAs, can I achieve higher growth by creating standardized SLAs – even if they help customers scrutinize my own operations more closely?
- ▶ Should I also provide service organization reports such as Statement of Accounting Standards No. 70 (SAS 70) or its successors, SSAE 16/ISAE 3402, which incorporate reporting on controls relevant to security, availability, processing integrity and confidentiality?

“An important overall issue is to get control of all your cloud usage – a CIO, for example, might not be aware that a sales department in another country is already using cloud services.”

Mal Postings

Global Advisory CTO – IT





“Right now, the issue of strategic sourcing is surrounded by the question of what is sensitive data, and very diligently weighing the pros and cons of putting that into the public cloud.”

Atul Sharma
Advisory – PI

Inhibitors

Inexperience

For vendor management, new approaches and skills are required, and new ways of thinking are needed for strategic sourcing. Because cloud computing is so new, however, most organizations have yet to develop the necessary experience and skills. “How you manage a vendor selling software licenses is very different from how you manage a cloud vendor that is selling on a pay-per-use basis,” explains Paul Chabot, Global Technology Industry, Advisory – PI. Practices that are well understood in terms of traditional outsourcing are unlikely to apply. Typical questions organizations must ask themselves in the context of clouds are, How do we maintain data quality and data integrity when the data is outside our walls? How are we going to assess the CSP’s security? What is the risk of data loss? Until there is more experience around these questions, they will be inhibitors to cloud adoption.

Re-thinking SLAs

Similarly, inexperience with negotiating SLAs for cloud services will inhibit adoption until companies figure out how to define appropriate service levels at each layer within the cloud model. Although SLAs

have traditionally related to the overall availability of service, including disaster recovery, cloud users have additional concerns because they typically lack other ways to enforce their requirements. “What information are you going to require that the CSP report back to you on an ongoing basis?” asks Atul Sharma, Advisory – PI. What clauses are you going to want in your service agreement to protect your business process? What penalties are you going to want if there’s a failure or if they can’t meet certain service level agreements, and how are you going to quantify the remedy? Even seemingly mundane issues can create challenges if they are not anticipated and processes agreed upon in advance. For example, CSPs must upgrade their infrastructure and perform maintenance from time to time. If the timing and scope of such activities are not defined and agreed to in advance, they might occur at a moment that interferes with a user’s critical business process.

Importantly, not all “down time” is equal in value: for example, an e-commerce site selling football apparel will lose more value during the Super Bowl in the US, or the World Cup in the rest of the world, than at any other time of the year. How will SLAs be written to account for such variability?

Complications for strategic sourcing

In terms of strategic sourcing, companies will need to think more about issues of data privacy, security, regulatory compliance, integration and misuse of data before they can make use of a public cloud service, as opposed to a private cloud or traditional outsourcing. Therefore, the sensitivity of the data involved will be an important factor in strategic sourcing analysis, including consideration of which applications and processes may be candidates for cloud services. Those activities that are lower-risk, and that cloud providers can do more cost-effectively, will move into the cloud. More strategic activities, which have higher risk around regulations, security and privacy, may remain in the private cloud or move more slowly into public clouds. This dichotomy is seemingly more evident for larger organizations; small- and medium-size companies are pursuing public cloud alternatives more broadly.

Dependencies, maturity rates and start-ups may all inhibit adoption

Because so many corporate IT infrastructures have grown piece by piece over many years, the system interdependencies in these environments sometimes are difficult to understand or define.

Therefore, which applications and processes are being considered for migration to the cloud may be further restricted depending on whether a company can determine those dependencies. "The cloud opportunity puts a spotlight on this issue; many companies will have a lot of homework to do before they can even take advantage of the cloud," says Atul. The dependency issue is exacerbated in situations where multiple cloud vendors are required to interoperate to address a given business process.

Sorting the "mature" cloud services from services that may not be ready for enterprise deployment is another challenge that may inhibit adoption. According to Atul, there is no shortcut for this issue; each potential service should be investigated at a deep level of detail and matched to the precise business requirements involved. Finally, another inhibitor is that enterprise customers know that with so many start-ups offering innovative cloud services, there is a high likelihood that many of them will not survive over the long term. For larger and more established organizations, potential savings and other benefits may not be worth the risk that a given provider will go out of business, while smaller organizations may be more willing to accept that risk given the potential cost savings.

Ernst & Young observations

In order to manage their CSPs on an ongoing basis, organizations will need precisely defined criteria for the information they wish to have regularly reported; service levels defined specifically in the context of an individual application or business process; and clear penalties articulated in the event of a service outage or failure to meet service levels.

Organizations that commit to cloud services may need to focus on deliberately shifting their staff from technical experts to people more skilled at managing vendor relationships.

As cloud service maturity levels evolve rapidly over the next few years, organizations will want to consistently revisit strategic sourcing decisions. The potential for migrating specific applications to the public cloud will change over time.

Organizations that determine that at least a part of their success comes from core competencies reflected in a legacy application might consider never putting that application in the public cloud.

Organizations should consider cyber risk liability insurance in their CSP contracts – it is a protection that is too often overlooked.

"As it becomes more common to have multiple vendors providing applications to support one business process, you're going to have higher risk profiles to manage."

Paul Chabot
 Global Technology Industry
 Advisory – PI



Drill-down discussion

Availability and interoperability

Sixty percent of the 1,059 North American and European business decision-makers surveyed are concerned about service availability in the cloud.¹

Current situation

Cloud computing promises flexibly scalable IT resources, low barriers to change, reduced capital expense risk and usage-based pricing, thus lowering an organization's IT costs, while freeing management to focus on building business agility, speed and innovation. None of these benefits are likely to be achieved, however, unless you diligently match the availability and interoperability attributes of a CSP to the requirements of your business. That's no easy task. Interoperability – enabling processes from different IT systems to work collaboratively or to share data – always presents formidable challenges, and it will be no different in the cloud.

Availability in the cloud

The common vision of cloud computing likens cloud services to power or landline telephony – “utility” services that are among the most dependably available services you can buy. Customers cannot simply assume, however, that any cloud-based service from any CSP will always be there every time they need it. Although the business models of the largest CSPs involve multiple data centers in different geographies, spreading and balancing

workloads among them, many do not. Often, CSPs have poor regional or global coverage that might affect a customer's experience – in other words, a given customer might be served from a single, potentially distant data center. Disaster recovery capabilities are, likewise, different from provider to provider and may not match the needs of all organizations. It's important to know how often a CSP does verification testing of its disaster recovery capabilities, and in what form it reports on such testing.



Further, lack of standardization and CSPs' efforts to differentiate their service offerings create issues for customers wishing to "recover" to a different cloud service, or to simply switch CSPs, as described by the European Commission.² Finally, it's important to understand how availability is affected, positively or negatively, by a CSP's "supply chain" – for example, a SaaS provider whose application is hosted by a platform or infrastructure service provider.

Interoperability in the cloud

CSPs and their customers must consider interoperability issues in many dimensions. Assuming that no medium or large organization will migrate its IT operations to a cloud model overnight, the biggest interoperability issues are likely to be those between the customer's existing infrastructure, data and applications and the CSP's. For example, a customer database migrated to the cloud may still need to interact with in-house marketing automation and ERM systems. "There will also be interoperability issues in orchestrating the efforts of multiple CSPs to provide a coordinated set of services that address a

single business process," says Paul Chabot, Global Technology Industry, Advisory – PI. Additional interoperability issues stem from the desire on customers' part to be able to move from one CSP to another, juxtaposed against the CSP's desire to "lock-in" customers – an issue that is also described in the European Commission report cited earlier.

Accelerants

Elasticity of the public cloud

Perhaps the major accelerant of public cloud adoption is its ability to elastically scale IT resource availability up – and down – depending on the momentary needs of the business. This resolves a long-standing dilemma for large organizations, which forecast demand for their IT resources yet typically end up with more capacity than they need – or worse, less than they need – because of business changes during the installation process. "Clouds promise to solve this issue by more closely aligning demand with supply," notes Amr Ahmed, Advisory – PI. Cloud-based IT services can grow or shrink as business requirements change, without requiring long implementation times or aggressive capital investment (see Figure 2, page 24).

"Alliances make a lot of sense because of the lock-in problem that customers face. We'll end up either with really open interoperability among CSPs, or more groups of alliances."

Hanny Kemna
 EMEA Advisory – IT

Questions to consider

Cloud business user

- Are my IT capacity requirements really so changeable that I need the high elasticity of public cloud services?
- Am I ready to pay a higher price for integrated tiered disaster recovery capability as part of my cloud service?
- Can I delineate the dependencies in my own data center well enough to coordinate hybrid services and processes that combine my own infrastructure with a CSP's?
- Have I assessed the comprehensiveness of my CSP's SLA provisions to ensure that they adequately cover the availability tolerances of my applications?
- How will I monitor the cost-effectiveness of my cloud solutions in order to determine if it ever makes sense to return to an in-house model?
- Am I prepared to deal with multiple CSPs to provide a single business service, or should I consider working with cloud "brokers" to orchestrate multi-provider services?

Cloud service provider

- How transparent can I be about the inner workings of my infrastructure? Does too much transparency increase vulnerability to cyber attack?
- What will create more value for my organization: customer lock-in or a demonstrated commitment to interoperability?

“Most SLAs lack detailed disaster recovery, because few buyers are willing to pay for it. However, this trend is changing today, as disaster recovery is nearing the top of the IT agenda.”

Amr Ahmed
Advisory – PI

Emergence of interoperability standards; superior resilience

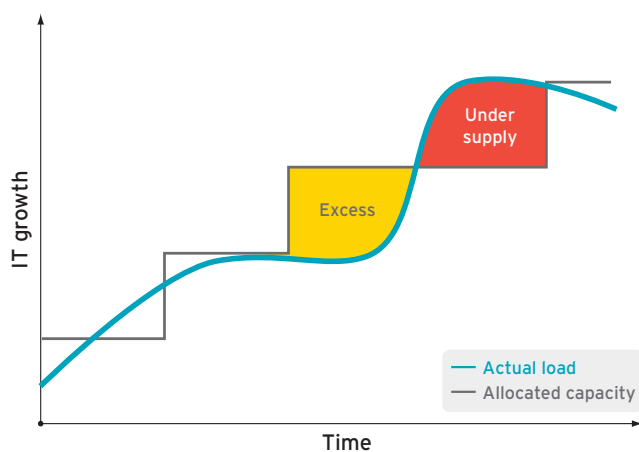
While interoperability standards are not yet mature, several coalitions of technology vendors, CSPs and service users have formed to drive the creation and adoption of such standards. Most include the word “open” in their name, such as the Open Cloud Consortium, the Open Cloud Manifesto, the Open Data Center Alliance and the Open Cloud Standards Incubator. They advocate the belief that widespread acceptance of interoperability standards is necessary to mainstream cloud adoption.³ “A factor that might help enable interoperability is that cloud services typically are based on virtualization technology, which is also being adopted inside corporate data centers,” notes Amr.

Further, interoperability standards would enhance availability, providing another potential accelerant. CSPs that can provide leading disaster recovery practices may be able to demonstrate resilience superior to that of an individual enterprise; by adding strong interoperability standards, CSPs could go further by providing “failover” capability from one cloud to another.⁴

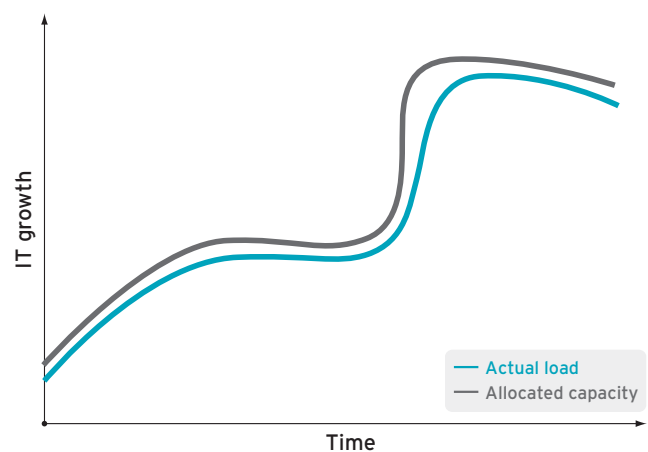
Some CSPs address availability through their own standard SLA provisions and processes, and a few have even established public websites that provide users with real-time insight into the status of their services. These leading CSPs view availability and security as among the most important issues for broad adoption, and the measures they are taking are effectively setting the standard for new entrants to be successful.

Figure 2: How the cloud computing model achieves superior supply and demand alignment

**Traditional IT resource capacity
(Utilization challenge)**



**Cloud view – transforming IT
(Align supply and demand)**



Source: Ernst & Young analysis.

Inhibitors

Lack of standards

The difficulty with all the standards activities described above is that they are brand new – and standard-setting is a lengthy process. Stated simply, the biggest inhibitor to mainstream adoption of cloud computing is that the cloud services market lacks widely accepted standards for availability and interoperability. When mature standards emerge, they will mitigate the inhibitors described below.

Previous success

As is often the case, previous success inhibits rapid adoption of future innovation. Large organizations have existing infrastructure that represents a significant investment in a set of applications and a specific IT architecture. For such business users, moving everything to the cloud all at once isn't necessarily feasible, even if it were desirable. Thus, the difficulty of achieving interoperability between cloud services and internal infrastructure, data and applications becomes a critical concern of cloud adoption. Adds Amr, "It's hard for large companies to get a clear picture of the services interdependencies in their own data centers, because of inherited legacy environments and a lack of automated discovery and correlation in most data centers." The problem is magnified if only a subset of a business process is migrated to the cloud – for example, the database portion of a sales management process.

Inhibitors at every CSP size; public network dependency; legal discovery

Two issues related to availability are a cloud user's ability to recover within the cloud itself and the ability to recover to a different cloud. Each brings different issues. For example, in terms of availability within a given cloud, larger CSPs typically won't provide much transparent visibility of their disaster recovery mechanisms. Smaller CSPs may be more flexible about meeting different customer requirements than larger ones, which are typically unwilling to negotiate changes to their standard agreements given the difficulty of altering their large infrastructures to meet non-standard requirements.

Another inhibitor is that the availability of public clouds is, by definition, at the mercy of public network performance, whereas an organization with its own private network can determine its own availability and performance requirements. Finally, cloud users must ascertain their CSP's ability to support "e-discovery," the process of locating and preserving data that relates to investigations and litigation. E-discovery has become a requisite for large organizations relatively recently, and it is not yet clear how cloud services will address it.

Ernst & Young observations

By understanding the different availability tolerances required by individual applications or business processes, cloud business users can negotiate varying levels of availability and pricing, as required.

Interoperability already is an important criterion because of the need to integrate cloud services with existing IT infrastructure, and because there are many start-up companies whose innovative cloud service offerings could be integrated with one another. As CSPs become more specialized, the importance of interoperability will increase as multiple CSPs become involved in supplying a given solution, whether that solution is orchestrated by in-house IT management or cloud service "brokers."

Due to the nearly infinite permutations that are possible in IT infrastructure, when it comes to interoperability standards there is no substitute for bilateral testing – direct tests between two parties. CSPs wishing to demonstrate their commitment to interoperability should consider bilateral testing, even with competitors.

"You need to understand the precautions your CSP has taken. If something is truly business-critical, you may want to ask the provider to take additional, specific precautions."

Paul Chabot
 Global Technology Industry
 Advisory – PI



Drill-down discussion

Security and privacy

“With regard to security issues, this is as much a cultural and mindset change due to loss of control, as it is an infrastructure change.”

Jose Granado
Advisory – IT

Current situation

While there is no doubt that cloud computing appears to be well on its way “across the chasm” to mainstream adoption, concerns over security and privacy slowed its early adoption.

Turning over control of the security of their IT infrastructure and data is an inherently uncomfortable situation for senior corporate managers – and it goes against the existing culture of many large corporate organizations. It’s no surprise, therefore, that a research survey of North American and European businesses found that 50% of respondents said their chief reason for avoiding cloud computing was security concerns.¹ In a separate global study of IT risk, 77% of respondents said adopting cloud computing makes protecting privacy more difficult.²

Security in the cloud

Culture and comfort aside, simply communicating data over the public internet, as opposed to keeping it entirely within a private corporate network, may increase data vulnerability. In addition, the business models of CSPs involve sharing infrastructure among many clients and managing IT workloads among many different physical machines or even geographically dispersed data centers. That workload management issue means that a given cloud user may not be able to determine precisely where its data is located or how that data is protected. The shared infrastructure issue effectively links the security fates of all users in a given cloud in a sort of unintended

commune. These issues were cited in a recent European Commission report as the key reasons why cloud computing will require entirely new security governance models and processes.³

Privacy in the cloud

On the privacy side, there is the concern, of course, that personally identifiable information stored in the cloud can be breached more easily than if stored in-house – but that’s mainly a security concern. Beyond data protection, the core privacy problem for enterprise businesses adopting cloud computing stems from the diversity of privacy regulations from country to country, juxtaposed against the CSP business model.

"Because the cloud is a virtual environment and data can be anywhere, you as a user may not know whether you are violating privacy regulations in the countries where you operate. And if the cloud data center is located in another country, you may not even know what country's regulations apply," explains Sagi Leizerov, Advisory – IT.

Accelerants

Security expected to rise as primary driver of cloud adoption

In the same research survey where 50% of respondents cited security concerns as their chief reason for avoiding cloud computing, Forrester Research projected that within five years, cloud security will become one of the primary drivers for adopting cloud computing.⁴ What could cause this shift?

In fact, there already is a growing minority view that using a CSP enhances security.⁵ A CSP's viability depends in part on establishing a reputation as trustworthy. Therefore, according to this view, the CSP will devote significantly more resources to security and data protection than a typical business, whose IT department is a cost center that often faces diminishing budgets. In fact, this is being seen already: leading CSPs view security as among the most important issues for broad adoption, and the measures they are taking are effectively setting the standard for others.

Additionally, the migration to using a CSP may galvanize centralization of enterprise data from across the business. "Having your data all in one place allows for better security management and the employment of consistent policies," says Jose Granado, Advisory – IT.

Emergence of leading practices and standards will promote the cloud

The main factors that could accelerate resolution of security and privacy issues associated with cloud adoption are leading practices, standards and cloud-specific regulation of security/privacy – all of which are slowly emerging from several regions around the world.

For example, the Cloud Security Alliance (CSA) is a non-profit organization formed to promote the use of leading practices for providing security assurance within cloud computing, for both cloud customers and CSPs. CSA's activities, initiatives and publications in this space include security guidance, a cloud security competency certification program and a suite of tools called "GRC Stack" for governance, risk and compliance in the cloud. GRC Stack offers, for example, a control set and an assessment questionnaire for cloud stakeholders.⁶

At the same time, the European Network and Information Security Agency (ENISA), commissioned by the European Parliament, is working to harmonize privacy law differences across the EU. Another ENISA initiative is to provide a benchmarking model to help cloud users compare CSPs on a consistent scale. "To enable the user to more efficiently compare different cloud service offerings based on a standardized set of controls or a set of audit tasks would be empowering," notes Thomas Loczewski, EMEA Advisory – IT.

Questions to consider

Cloud business user

- What is my organization's risk tolerance?
- Which compliance and security requirements must be met?
- How can my CSP help my organization comply with the varying data privacy rules in all of the jurisdictions where I do business?
- What independently verifiable assurances of security and privacy does my CSP offer?
- What security and privacy metrics will I use in selecting a CSP, and how will I monitor them?
- How will I maintain data quality?
- How will I set up my sourcing governance for a CSP landscape?

Cloud service provider

- Which compliance and security requirements of the customer need to be met?
- How can I comply with varying data privacy regulations, while maintaining a virtual cross-border business model?
- What independently verifiable assurances can I offer cloud users of agreed-upon security and privacy levels?
- How can I balance the transparency of my operations with security for cloud users?
- What policies can I offer cloud users related to security/privacy breaches, and what remedies am I bound to?

US government legislation is expected to accelerate the resolution of security and privacy issues in cloud computing, indirectly and directly. Health care reform and stimulus funds earmarked for the application of technology to health care administration processes as well as the E-Government Act require standards to be adopted to promote the seamless and secure flow of data. Moreover, as the US government continues to increase its usage of cloud services, it will push the development and implementation of standards and regulation. For example, the Federal Risk and Authorization Management Program (FedRAMP) has been established to provide a standard approach to assessing and authorizing the security of cloud computing services and products for US government agency use.⁷ In late 2010, US agencies began awarding cloud services contracts, including a General Services Administration (GSA) award to a team led by Unisys and Google and a Department of Agriculture award to Microsoft. Both deals include email and other collaboration applications.^{8,9}

Virtualization's rapid adoption promotes private clouds

Finally, there is the relatively rapid adoption of virtualization technologies inside the firewalls of corporations, essentially creating private clouds. Because private clouds are under the direct control of a company (even though a third-party firm may manage them), they are not subject to all of the inhibitors affecting the adoption of public clouds. They can provide an interim step, however, that helps to prepare a company for rapid migration to lower-cost public clouds once risk management and data type classification have been appropriately aligned with compliance requirements and sourcing options.

Inhibitors

Loss of control

Loss of control is rapidly emerging as the number one inhibitor to adoption of public cloud computing services. According to *Borderless Security: Ernst & Young's 2010 Global Information Security Survey*, "many companies are concerned about giving up control of access to their business information and relying on the cloud to provide secure authentication, user credentials and role management."¹⁰

Even in traditional outsourcing, the enterprise doing the outsourcing typically maintains responsibility for security, or at least co-manages it. Other than establishing and enforcing policies such as password changes, however, CSP business models essentially place all responsibility for security on the CSP. And the same business model issues can limit the transparency of the CSP's security measures. In a related issue, it's not always clear how an organization can maintain single sign-on for authentication across in-house and cloud systems.

Still, the Ernst & Young security survey found that 45% of its 1,598 respondents from 56 countries have either deployed or are evaluating cloud computing, "a surprisingly high number given that the reliability and security level of many cloud services is still unknown." To get comfortable with cloud services, companies often require granular detail about how their information is protected by the CSP. Security audits are a typical information security best practice, but a CSP's ability to respond to security audits is sometimes limited if its business model virtualizes operational details in order to gain efficiency and provide ease of use to customers. To help mitigate these concerns, many CSPs are utilizing assurance programs such as SAS 70 (to be succeeded by SSAE 16/ ISAE 3402), International Organization for Standardization (ISO) 2700X and Trust Services, which provide standardized reporting on security practices.

"It's counterintuitive for security officers, who have been responsible for protecting an organization's data and intellectual property, to give up control of infrastructure and data to a third party."

Jose Granado
Advisory – IT

CSPs are attractive targets; cross contamination concerns; protecting personal information is key

Other inhibitors include the concern that CSPs may be more of an attractive target for hackers than an individual company, because multiple companies' valuable data is housed with the CSP. Another is the risk of cross contamination, i.e., the potential for one user of a cloud service to gain access to another's data. The European Commission report cited previously noted both these concerns.

Protecting the privacy – i.e., the personally identifiable data – of employees, customers and business partners is already a challenging proposition for multinational corporations. Privacy attitudes and regulations differ, sometimes significantly, from jurisdiction to jurisdiction – country by country throughout the EU and Asia-Pacific regions and state by state in the US. Privacy becomes exponentially more complex if a company turns over its data to a potentially borderless CSP. This has led to a call for countries to “harmonize their laws on cloud computing” to reduce inconsistencies in regard to privacy and security.¹¹

Understand the implications of what you are moving to the cloud

Before migrating any servers, databases, applications or data to the cloud, companies should evaluate the nature of the information they would be moving, the sensitivity of that information and whether the CSP's service location is appropriately secure for that information to reside. Before companies proceed, they should consider potential consequences from the fact that any sensitive data placed in the public cloud may become subject to the regulations of an unknown jurisdiction, especially if they are dealing with a CSP that does not make its data center locations known.

For example, if a European company's data is stored in US data centers by its cloud provider, it becomes subject to the USA Patriot Act. That law allows the US government to access data stored within US borders.¹² “Because you are in a virtual environment and data can be anywhere, a business user must be aware of all the different borders its data is crossing and the regulations that apply from each of those countries,” explains Bill Schaumann, Advisory – PI. While placing restrictions on where data can reside and travel seems like an easy fix, a CSP may not be able to comply with such restrictions. If it can, the restrictions will likely cause an increase in the price of the service, reducing the value of migrating to the cloud.

Deleted data doesn't necessarily disappear

Finally, CSPs and their clients alike need to be concerned with the fact that data sometimes persists in servers through which it has traveled, even after having been “deleted.” “Underlying all the security and privacy issues is the concern that once it is shared, it will persist in that environment forever,” says Paul Chabot, Global Technology Industry, Advisory – PI.

Ernst & Young observations

Except where CSPs can demonstrate the necessary security and privacy measures, the safest way for large organizations to explore cloud services may be to build internal private clouds for applications involving sensitive data, while simultaneously investigating public clouds using non-sensitive data. It's important to explore public cloud services in order to be ready to adopt these economically advantageous models as soon as their risk management and data type classification has been appropriately aligned with your organization's compliance requirements and sourcing options.

To overcome the security and privacy issues of cloud adoption, buyers of cloud services can approach the move with thorough diligence that matches their risk posture, and also matches security and privacy requirements to the risk posture, service level agreements and demonstrated capabilities of the provider.

The potential for breach necessitates that the CSP and business user come to an agreement up front about notification and remedy policies.

CSPs should provide for internal and external security audits.





Drill-down discussion

Standards and risk management

Risk management is under-addressed: only 36% of US and 57% of EU survey respondents agreed that their organizations are vigilant in auditing and assessing the risk associated with planned cloud offerings before adoption.¹

Current situation

Anytime you relinquish control, you add a measure of risk to your situation. For IT users, balancing the levels of risk and opportunity within their business is a significant task that is added to and changed in important ways when migrating to a CSP. Industry standards are among the key mechanisms that help mitigate risk.

From a risk management perspective, the main changes when moving from in-house IT infrastructure to cloud services are in the areas of data security and privacy breaches, as well as regulatory and legal compliance. Cloud computing is also likely to change certain non-IT ERM issues as well, although its impact is not yet well understood. Industry standards, often a risk management safety net, are lagging behind the rapid growth of cloud services. The lack of specific standards, especially in the areas of security, privacy and availability, is often cited as a barrier to industry growth, because without standards, cloud users have a high degree of uncertainty about the risks they are assuming.

Many government, industry and public-private coalitions are racing to fill the standards void and thus ease risk management for CSPs and their users. Standards development, however, is a consensus-driven and therefore lengthy process – especially for international standards such as those being developed for cloud computing. Because cloud computing is a relatively recent phenomenon, the cloud standards process has begun only recently.

Accelerants

Focus on standardization initiatives

Many standardization initiatives are under way, with the intent of helping companies transition to the cloud by providing assurances that help users manage their risk. Although cloud standards are being developed globally, the US NIST has been recognized as a leader in cloud standards development. NIST's widely accepted definition of cloud computing is referenced in a European Commission cloud report² and reprinted in a technical report from the European Telecommunications Standards Institute (ETSI).³ The full NIST definition of cloud computing is included in the Glossary (see page 52).

The NIST views itself as a catalyst in helping the industry create its own standards, with the goal of promoting government and industry adoption of those standards.⁴ The NIST is in the process of launching an online portal to identify gaps in cloud standards to accelerate the development of standards for security, interoperability and portability. The NIST points out that the product of these initiatives must walk a fine line between being definitive enough to be useful without being so overly specific as to retard innovation.⁵

Multiple coalitions are driving standards efforts

Other efforts from many supplier-driven, user-driven and combined organizations are also under way. Important global standards development organizations (SDOs) include the Distributed Management Task Force (DMTF), the CSA, the Object Management Group (OMG) and the Open Cloud Consortium (OCC), all of which include members from dozens of countries around the world.^{6,7,8,9} While some SDOs are narrowly focused, such as the CSA on best practices for cloud security assurance, most are developing multiple different standards meant to address interoperability issues among multi-vendor clouds or between clouds and in-house systems and data. Their output consists of standards specifications, reference implementations and benchmarks. The DMTF and CSA are expected to publish draft specifications in 2011.

Questions to consider

Cloud business user

- ▶ How is my cloud strategy integrated into my ERM activities?
- ▶ What processes and controls are in place for security occurrences or incident reporting and resolution?
- ▶ How and how often will I measure my CSP's adherence to agreed-upon service levels/standards?
- ▶ How will I test cloud offerings? What are the right pilot projects?
- ▶ What is my organization's risk tolerance profile?
- ▶ What measures are being undertaken by my CSP to address availability and security, including audits to address compliance with NIST/SAS 70 (or its successors, SSAE16/ISAE 3402) standards?
- ▶ Do I have the processes in place to update my services to reflect regulatory and standards changes across the globe in a timely manner?

Cloud service provider

- ▶ How will I stay current with the perceived risks that have an impact on my business?
- ▶ What type of assurance will I provide my customers, at what intervals and at what cost?

"Cloud users are worried about the potential for security and data privacy breaches, in addition to worrying about whether they are violating any regulations or compliance rules."

David Roque
Advisory – IT





“Standards will likely be developed over the next 18 months to 2 years, with refinement thereafter as cloud users continue to become more aware of the issues they need to have addressed.”

Hugh Rosengarten
Advisory – IT

Interoperability versus vendor lock-in

Besides finding the right path between useful standards and continued innovation, many of these standards efforts must deal with the opposing forces of interoperability and vendor lock-in. Cloud users wish for the freedom to switch easily among CSPs, which lowers risk; but CSPs’ risk is lowered by proprietary ties that bind customers to their particular systems. Complicating interoperability issues is that high-value innovations are, by their nature, proprietary to the CSPs that created them.

Inhibitors

Fear of the unknown

While some believe that the risks inherent in cloud computing are the same as simply using the internet – namely, exposing your systems and data to cyber attack or other unauthorized or criminal access – many organizations have a more prevalent overall risk anxiety about the cloud, fueled in part by fear of the unknown. “With traditional outsourcing, there are many of the same risks, but the physically tangible nature of the third party and the longer history of those relationships help businesses understand the risk analysis better,” explains David Roque, Advisory – IT.

Thinking beyond straightforward IT-related risk, migrating to cloud computing is likely to have an influence on a broad range of organizations’ more traditional ERM considerations, such as legal liabilities, regulatory compliance and brand protection and the need to refocus and restructure their internal IT organization, among others (see Figure 3, below). For example, risk managers must understand how the risk of brand damage might change if control of a customer-facing website is migrated to a CSP instead of being administered in-house. There may even be risks to consider in not migrating to cloud computing rapidly enough – e.g., if the cloud paradigm catches on fast and if cloud-based competitors gain advantage through faster access to the latest advanced technologies. Such questions have only recently been raised, and most companies have not yet begun to consider them.

One way in which some organizations have tried to minimize risk is to migrate only non-core functions and non-sensitive data to the cloud initially. For example, the US government migrated its Recovery.gov website, which provides public access to information about the use of economic stimulus funds. That approach, however, can mitigate only certain risks, such as data security and compliance with privacy regulations.

Figure 3: Cloud security “threat matrix” guidelines

1. Organizations shall develop and maintain an ERM framework to manage risk to an acceptable level.
2. Formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods. A similar assessment should be done for inherent and residual risk, considering all risk categories (e.g., audit results, threat and vulnerability analysis, regulatory compliance).
3. Risks shall be mitigated to an acceptable level and time frame, which shall be established and documented with executive approval.
4. Risk assessment results shall include updates to security and privacy policies, administrative procedures, standards and controls to ensure that they remain relevant and effective.
5. Once access risks have been identified and prioritized, a plan should be put in place to minimize, monitor and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls should also be implemented prior to provisioning access.

The risk guidelines above are described in the CSA’s “threat matrix” – officially the Cloud Controls Matrix – a pragmatic tool to help CSPs address risk management concerns.

Source: CSA Controls Matrix web page, <http://www.cloudsecurityalliance.org/cm.html>

Immature standards

In the absence of definitive standards, current efforts to address risk management are disjointed and inconsistent; there is no agreed-upon baseline, creating a nebulous situation for CSPs and cloud users alike. Cloud users have turned to standards originally created for different purposes. For example, some require CSPs to provide SAS 70 reports. SAS 70 was defined by the American Institute of Certified Public Accountants (AICPA) and was originally geared toward financial controls.¹⁰ More popular in EMEA is ISO 27001 certification – or more officially, ISO/IEC 27001:2005, published by the ISO and the International Electrotechnical Commission (IEC). ISO 27001 generally is considered to be a better assurance tool for cloud computing services because it is focused on security, but it is sometimes criticized for lacking sufficient testing of the security environment and controls in operation. Another emerging assurance reporting standard is International Standard on Assurance Engagements 3402 (ISAE 3402), put forth by the International Auditing and Assurance Standards Board (IAASB).

Meanwhile, a proposed security standard from the US NIST, described in Special Publication 800-125, *Guide to Security for Full Virtualization Technologies (Draft)*, is being evaluated by many CSPs for certification efforts because it has more comprehensive detail than many others. “The standard actually has very specific details such as level of encryption, and the type of technology used. It drills down to a level where someone could say, ‘I understand that the right safeguards are in place,’” David explains.

Under these circumstances, it is not surprising that many believe the cloud market is still too immature for standardization, so CSPs and their customers must make do with the tools they have, recognizing that they may be imperfect (see Figure 4, below). According to Forrester Research, CSPs’ practice of adhering where appropriate to previously accepted standards has so far mitigated some of the trust issues resulting from the immaturity of current cloud standards.¹¹

Ernst & Young observations

The decision to embrace cloud computing technology should include a risk-based analysis that includes all aspects of the business; it is not simply a technology decision.

The dearth of specific cloud computing standards is somewhat mitigated because most CSPs have developed their technologies adhering to prior standards in areas such as security, networking and protocol standards.

CSPs can help address risk management by offering more “thought leadership” in the form of educational materials that provide context for their approach to the standards and risk management issues that are the most important to their customers.

Figure 4: Some possible future standards

1. Federated security (e.g., identity) across clouds
2. Metadata and data exchanges among clouds
3. Standards for moving applications between cloud platforms
4. Standards for describing resource/performance capabilities and requirements
5. Standardized outputs for monitoring, auditing, billing, reports and notifications for cloud applications and services
6. Common representations (abstract, APIs, protocols) for interfacing cloud resources
7. Cloud-independent representation for policies and governance
8. Portable tools for developing, deploying and managing cloud applications and services
9. Orchestration and middleware tools for creating composite applications across clouds
10. Standards for machine-readable service level agreements (SLAs)

If all the cloud standards on this wish list were achieved, cloud users would fully realize the cloud’s potential for IT flexibility and scalability that enables business agility. They are unlikely to be realized quickly, however, given that the wish list would limit CSP differentiation.

Source: Cloud Standards Overview, Object Management Group, July 2009, http://cloud-standards.org/wiki/index.php?title=Cloud_standards_overview

Drill-down discussion

Government

The US federal government is the world's largest IT buyer, spending more than \$76 billion each year on more than 10,000 systems.¹

Current situation

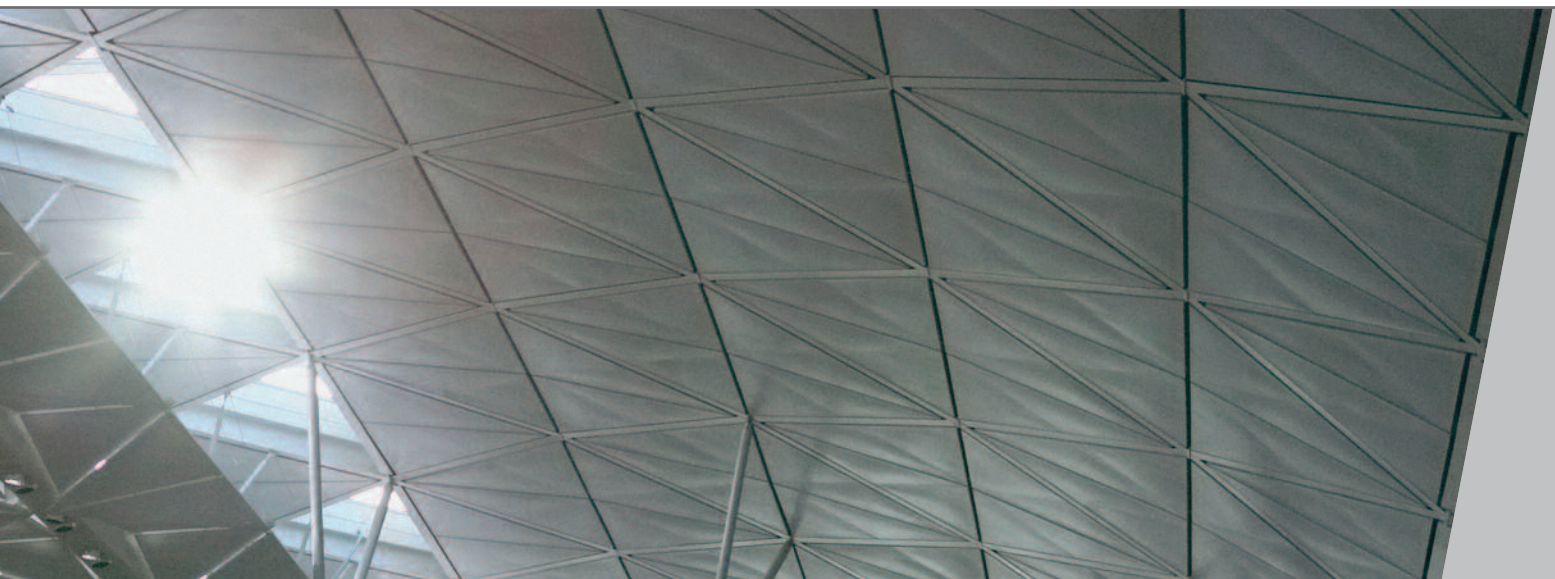
Governments around the world are actively pursuing cloud computing for their own use. Some pursue it for the same benefits being sought by private companies: lower cost, increased agility and reduced energy consumption. Some pursue it as a source of economic development, hoping to create leading cloud development and service centers within their borders. And many nations look to achieve both these ends.

At the same time, however, critical factors impede government pursuit of cloud computing. Governments have a high degree of concern about the security, privacy and data location issues that come with cloud computing. Governments are often decentralized, with IT usage and purchase authority distributed among dozens, hundreds or even thousands of agencies. Finally, governments are sometimes slower than the private sector in adapting to change – and change is rampant in cloud computing, because it is still rapidly evolving. These can be difficult challenges for CSPs wishing to do business with government agencies.

Government cloud initiatives

While there are many more government cloud computing initiatives than we can list, the following highlights demonstrate the intensity with which governments are embracing the cloud.

The US federal government is perhaps the most active. Aneesh Chopra, the US Chief Technology Officer, and Vivek Kundra, Chief Information Officer (CIO) of the US, are both frequent public speakers in support of cloud computing. “Over the past decade, the number of federal data centers has grown from 432 to more than 1,100.



This growth in redundant infrastructure investments is costly, inefficient, unsustainable and has a significant impact on energy consumption,” Kundra said in an April 2010 speech to the Brookings Institution about the future of cloud computing.² Among the US initiatives that aim to address those challenges through accelerated adoption of cloud services are:

- ▶ Apps.gov, an electronic SaaS “marketplace” for federal agencies provided by the GSA.
- ▶ The FedRAMP, which aims to “promote faster and cost-effective acquisition of cloud computing systems by using an ‘authorize once, use many’ approach to leveraging security authorizations.”³
- ▶ Standards-setting efforts by the NIST.

- ▶ Leading by example: the migration of multiple websites and IT infrastructures to public cloud environments, including Recovery.gov, which provides public access to information about the use of economic stimulus funds.
- ▶ Multiple cloud contracts awarded late in 2010 – with more believed to be on the way – including a GSA award to a team led by Unisys and Google and a Department of Agriculture award to Microsoft. Both deals include email and other collaboration applications.^{4,5}

“Heightened concern about security, privacy and jurisdictional authority will always be an issue for any government, whether the cloud service involved is provided via public or private infrastructure.”

Nick Son

Advisory – Government and Public Sector

Questions to consider

Cloud government user

- ▶ What do I have to do, in my contracts and in my technical implementation, to avoid long-term vendor lock-in?

Cloud service provider

- ▶ Given the experience necessary to do business with government agencies, who can I partner with that can provide that experience and fit well with my organization?
- ▶ Does it make sense for my organization to contribute to the economic development of a region where we intend to do business?
- ▶ Will my staff withstand the scrutiny required for security clearances necessary to conduct government business with sensitive data?
- ▶ Can my infrastructure provide the transparency governments require for monitoring controls?
- ▶ Am I prepared to help governments develop the strategic business cases necessary to justify investments in the cloud?

“Adaptation to regulatory requirements is difficult everywhere. In Europe, each nation implements EU regulations independently. Across the US, each state and the counties in them have their own nuances to their privacy requirements.”

Werner Lippuner

Advisory – Government and Public Sector

European Union in the cloud

The EU's pursuit of cloud computing can be seen in the European Commission's two main cloud computing recommendations from a January 2010 report: the first recommendation is to stimulate cloud research and development within member states; the second is for member states to work together with the European Commission to “set up the right regulatory framework to facilitate the uptake of cloud computing.”⁶ The UK government has gone further by defining and beginning to move its IT infrastructure into a “G-cloud,” or Government Cloud.⁷

China and Japan in the cloud

The Japanese government also is attempting to lead by example. Its Digital Japan Creation Project challenges the nation to take leadership roles in several technology areas, and identifies the “Kasumigaseki Cloud” as a project in which the government will “take the initiative.”⁸ The Kasumigaseki Cloud is intended to provide IT infrastructure to multiple Japanese ministries, and to provide e-government to the nation as well.

The Chinese government announced in October 2010 that five cities – Beijing, Shanghai, Shenzhen, Hangzhou and Wuxi – would host cloud computing innovation centers with the aim of developing them into leading centers of cloud technology.^{9,10}

Security, privacy and compliance

Not surprisingly, the high-level obstacles to government adoption of cloud computing mirror those of any large organization. For example, one of the most critical issues is identifying sensitive data and safeguarding it better than non-sensitive data, which directly affects the choice of projects to pilot in the public cloud. Says US CIO Kundra: “There's a huge difference between a government infrastructure in the cloud and putting a website like Recovery.gov, a consumer-facing site, in the cloud.”¹¹ Werner Lippuner, Advisory – Government and Public Sector, agrees: “Around the world, governments eager to engage with cloud services are beginning with low-risk, consumer-facing services. Thus, they are gaining experience for future deployments with more sensitive and nuanced requirements.”

“Cloud computing systems don't ever have a status quo; they are constantly evolving. The challenge for governments is to define regulations that are truly reflective of this cloud characteristic.”

Dhavan Mehta

Advisory – Government and Public Sector



Other governments make similar distinctions in their cloud plans. However, that does not prevent military and intelligence branches from exploring cloud initiatives. For example, the US Central Intelligence Agency has stated its enthusiastic support for cloud computing – although it intends to use its own private cloud.¹² “Each government agency will need to develop safeguards that are appropriate to its own individual mission,” notes Dhavan Mehta, Advisory – Government and Public Sector. However, Dhavan points out that the success of cloud-based services is as inevitable in government as it is in the private sector – and for similar reasons. Agencies are attracted to the pay-as-you-use versus install-and-own business model to manage costs, to enable flexible and fast response to ever-changing technology and to redirect resources to focus on delivering value.

Governments are particularly concerned with the privacy of their citizens, which leads to strict regulations with regard to personally identifiable data as well as data location. Many of the government plans cited above include expectations that cloud

vendors will enable them to know precisely where their data is stored, something they acknowledge is not always the case at present despite regulatory requirements. Of course, compliance with each government’s regulations is a requisite for doing business with them.

Are global regulatory agreements possible?

Yet some believe that governments should work together toward more universal agreement on such regulations in order to ease cloud adoption and accelerate their own access to cloud computing benefits. The Brookings Institution recently found that, in order to achieve the full potential of cloud computing, “countries need to harmonize their laws on cloud computing to avoid a ‘Tower of Babel’ and reduce current inconsistencies in regard to privacy, data storage, security processes and personnel training.”¹³

“If governments were to adopt cloud computing in a complete and holistic sense, the benefits have the potential to be greater than for any other type of organization,” says Nick Son, Advisory – Government and Public Sector.

Ernst & Young observations

Interoperability standards to enable vendor switching appear to be an even higher priority for government than it is for private companies, which can decide to allow themselves to be locked in if they see appropriate value.

Given budget constraints facing most governments, having the flexibility of a pay-as-you-go spending model, and the flexibility to expand and contract services quickly, makes good “mission sense.”



Drill-down discussion

Accounting

Worldwide revenue from public IT cloud services exceeded \$16 billion in 2009 and is forecast to reach \$55.5 billion in 2014.¹

Current situation

Surging use of cloud computing has led to an increased awareness of the many practical complexities inherent in accounting for cloud services transactions. Part of the attraction of cloud services is their turnkey and multifaceted nature, potentially offering cloud users a fast and easy way to integrate applications, platforms and infrastructure. Additionally, CSPs' service offerings enable businesses to subscribe to a wide variety of application-related services that are developed specifically for, and delivered over, the internet on an as-needed basis, many times with little or no implementation services required and without the need to install and manage third-party software in-house. However, this very service delivery model often creates accounting challenges for CSPs, particularly around revenue recognition and the treatment of certain costs.

Understanding the guidance

Revenue recognition

"Much of the available revenue recognition guidance predates the rise of cloud computing and was conceived with product companies in mind more than service companies," notes Alex Bender, Technology Industry – Assurance. Applying this guidance can be complicated, especially when there are multiple elements included in the cloud service arrangement.

Generally, little specific guidance exists on the accounting treatment of service arrangements. As a result, the general

revenue recognition criteria in Accounting Standards Codification (ASC) Topic 605-25 and Staff Accounting Bulletin No. 104 (SAB 104), and the multiple-element guidance in ASC 605-25, should be applied by companies when accounting for service transactions not expressly addressed by other authoritative literature. Under these rules, revenue for service transactions should not be recognized before a contract exists, services are provided (delivery occurs), amounts to be received as compensation for the services performed can be objectively determined (fees are fixed or determinable), and the fees are collectible or realizable.



While the revenue recognition for stand-alone cloud services arrangements may generally be straightforward, complexities arise when multiple elements are bundled. This is often the case for CSPs' arrangements, which may include the cloud services, hardware or some other product or service (including professional services) that was bargained for as part of the arrangement. In order to assess the appropriate revenue recognition for a cloud services arrangement, the CSP must first identify all of the deliverables within the arrangement. Once the deliverables have been identified, the CSP must determine which deliverables may be treated as separate units of accounting and allocate the transaction consideration to those units of accounting. Given that most cloud revenue arrangements are recognized ratably over the service period, cloud vendors can get lulled by the idea that revenue recognition is simple; however, evaluating the nature of the contracts can be quite complex, as seen by recent restatements by cloud vendors due to incorrectly considering all the terms of the arrangements.

Determining whether elements within a cloud services arrangement may be accounted for as separate units of accounting is a matter of professional judgment, and the facts and circumstances of each arrangement should be considered. ASC 605-25 provides specific criteria that must be considered in making this judgment.

If multiple deliverables included in an arrangement are separable into different units of accounting, the multiple-element arrangements guidance in ASC 605-25 addresses how to allocate the arrangement consideration to those units of accounting. ASC 605-25 requires the arrangement consideration to be allocated at the inception of the arrangement to the identified separate units of accounting based on their relative selling price (relative-selling-price method).

Questions to consider

Cloud business user

- ▶ How do I treat costs incurred to implement the cloud services (capitalize or expense)?
- ▶ How will my decision to migrate to the cloud impact key financial metrics (e.g., EBITDA, my loan covenants, analyst communications)?

Cloud service provider

- ▶ How can I identify, value and recognize each component of my bundled offerings?
- ▶ How should I treat direct and incremental costs?
- ▶ How will I monitor changing guidance?
- ▶ What are the accounting impacts of my SLAs?
- ▶ Given potential accounting complexity, are my financial results sufficiently comprehensible and transparent to investors and analysts?



“While identifying and valuing the different revenue elements may be complicated, timing of recognition may be more straightforward,” says Andrew Cotton, Technology Industry – Assurance. In most cases, existing guidance will lead to recognition on a pro rata or straight-line basis over the term of the agreement, although there may be cases where the specific agreement indicates a different pattern.

International guidance

For companies that report based on International Financial Reporting Standards (IFRS), the key pieces of guidance are similar in concept to US GAAP, but do not have specific implementation rules. As a result, non-US companies are encouraged to consider this guidance, because it is consistent with the IFRS principles involved and provides prescriptive guidance in areas where IFRS is silent.²

Direct costs

To defer or not to defer is often the question for CSPs when dealing with direct costs. Because most CSPs recognize revenue over the duration of the service period, they typically incur direct costs before revenue is recognized. For example, sales commissions are generally paid to the salesperson up front based upon the total value of the cloud service arrangements; however, the revenue from that arrangement is recognized over the underlying service period. As a result, CSPs that expense these costs as incurred, while recognizing the revenue over a period of time, are likely to report uneven profit margins over the cloud service term. Accordingly, CSPs often consider whether it is more appropriate to defer these costs and recognize them at the time the associated revenue is recognized.

Based on this guidance, we believe that although costs associated with a delivered item may almost always be expensed as

“The primary accounting issues that CSPs deal with are revenue recognition and the treatment of related costs.”

Alex Bender
Technology Industry – Assurance



incurred, these costs may be capitalized if 1) they create an asset or add to the value of an existing asset; 2) accounting for these costs is not specifically addressed by other authoritative literature, and the vendor has adopted and consistently applies a policy of deferring such costs in a transaction that results in the deferral of revenue; 3) the vendor has an enforceable contract for the remaining deliverables; and 4) delivery of the remaining items included in the arrangement is expected to generate positive margins, allowing realization of the capitalized costs. It is important for CSPs to carefully evaluate this guidance when considering the accounting for direct costs, as the types of costs eligible for deferral are different under both models. CSPs should also closely monitor the evolving accounting guidance in this area.

Costs incurred to develop internal-use software

Given the nature of the CSP's service delivery model, the underlying technology developed by the CSP will be used internally to deliver the service to its customers. Therefore, the associated cost to develop the software is generally accounted for

pursuant to ASC 350-40, *Internal Use Software*. Under this guidance, costs incurred during the preliminary planning and the post-implementation/operation stages are expensed as incurred. However, certain internal and external costs incurred during the application development stage may be capitalized provided certain criteria have been met. These capitalized costs would then be amortized over the estimated useful life of the technology and periodically evaluated for impairment.

Looking ahead

As cloud computing vendors are evaluating the effects of current US GAAP, they should be aware that additional changes to the revenue recognition guidance may be coming. The FASB and IASB continue to develop their joint project for a single revenue recognition model that would apply to contracts with customers. The Boards issued an exposure draft of a converged revenue recognition standard on 24 June 2010 and are anticipating the release of a final converged revenue recognition standard in 2011, with an effective date of 2014 or 2015 likely. Furthermore, the exposure draft may change how companies account for deferred costs.

Ernst & Young observations

Revenue recognition requires careful contemplation in light of a CSP's commercial offerings. There is no "one size fits all" approach.

Longer service contracts make revenue recognition for CSPs (in many cases) more predictable, which makes forecasting and revenue expectations easier. However, depending on the treatment of direct costs, CSPs may see revenue recognized much later than when direct costs are incurred and expensed.

Determining how to reflect direct expenses is best done conservatively and consistently on a case-by-case basis.





Drill-down discussion

Cross-border taxation of CSP arrangements

“Cloud computing is borderless by its very nature. One thing is certain, however – the world’s taxing authorities have not issued definitive guidance for its taxation; moreover, the business nature of the overall offering is also evolving, which creates further technical uncertainty as well as timing uncertainty as to when taxpayers can expect actual guidance. Companies are forced to make decisions based on current rules and interpretations across all relevant jurisdictions, but will likely nonetheless encounter tax surprises.”

Channing Flynn

Global Technology Industry Tax Services Leader

Current state

Cloud computing is often borderless, but tax regulations and tax compliance requirements are not. That simple-sounding conflict can give rise to complex and potentially material or significant tax issues, mainly for CSPs. To date, at least, in the evolution of cloud computing, most jurisdictions view CSPs as the responsible party for tax purposes regardless of any arrangements struck between CSPs and their users.

Sometimes CSPs are truly global “clouds,” providing limited or no transparency about where data is being processed and stored. More often, however, cloud service is provided by a group of interrelated but distinguishable data centers in different locations. It is important to understand this underlying point, because especially in the latter case, it means that both the CSP and the cloud user may be subject to all or some tax regulations in all of the jurisdictions through which the cloud network passes the user’s information.

“In general, under current rules the critical taxation issues in cloud computing are determining the character of CSP revenue and whether the CSP has a taxable presence (known as “nexus” in the tax world) in each of the jurisdictions in which the CSP does business,” explains Jeff Levenstam, International Tax. Both issues need to be separately sorted for income tax and indirect tax (sales, use, or value-added taxes) purposes, as different rules may apply. For tax compliance, the key issues are determining which regulations apply as a result of where a CSP’s data centers are located, as well as the level of support the CSP provides in meeting those compliance requirements. Other critical issues, such as transfer pricing, i.e., making decisions about the attribution of value or risk in a CSP model, and recent rules governing the disclosure of tax uncertainties, create even more ambiguity for taxpayers and the need for careful evaluation.

Cloud computing – general tax considerations

“One challenge in dealing with cloud computing taxation issues is that CSP business models are developing much more rapidly than the global taxing jurisdictions can respond with guidance,” explains Drew Alltizer, Tax. For example, the CSP must determine whether its revenue is characterized as revenue from a service or as revenue from a software sale or lease or perhaps a bundled package. The characterization can have a significant impact on whether sales or withholding taxes might apply, as well as determining the source from which revenue is earned (e.g., whether from foreign or domestic sources, which is relevant for determining home country taxation).

Currently, CSP revenue characterization is regulated inconsistently around the globe, and even state-by-state within the US. The Organisation for Economic Co-operation and Development (OECD), a peer group of 34 countries that provides a forum for governments to seek solutions to common issues, has issued a general statement that CSP revenue is more akin to revenue from a

service. However, the OECD’s guidance is non-binding; each country adopts its own laws and regulations, and the reality is that some characterize CSP revenue as a service where others treat it as a software sale or lease. “Making the distinction has significant and complex ramifications for all CSPs in terms of an overall tax mitigation strategy – especially US multinationals operating abroad or other multinationals operating in jurisdictions with similar worldwide taxing systems,” says Jeff.

From a US multinational’s perspective, the revenue characterization question impacts whether the income of the foreign subsidiaries is eligible for deferral from current taxation in the US, as different rules (including different exceptions) apply to services income versus licensing or leasing income. The revenue characterization is also extremely important for US state and local tax purposes, since services are generally not subject to sales tax, although various US states are starting to identify exceptions. Currently, 12 US states impose a sales tax on digital goods, and another 17 states were considering legislation during 2010 to impose a sales tax on digital transactions.¹

Questions to consider

Cloud business user

- ▶ Have I adequately considered tax nexus and the related compliance issues in the selection of my CSP, and are they clearly documented in our agreement? Are the filing and tax responsibilities clearly identified among the parties?
- ▶ How will I monitor CSP adherence to agreed-upon compliance duties?
- ▶ How will the relationship with my CSP adapt to changing tax statutory and regulatory requirements?

Cloud service provider

- ▶ Is my tax strategy aligned with my business model and flexible enough to change as required?
- ▶ Where do I have tax nexus?
- ▶ What are the revenue characterization and sourcing rules for each jurisdiction in which I operate? Do I have tax risk with respect to these issues?
- ▶ Am I aware of all potential domestic and global incentives to supplement cloud service provider expansion plans?
- ▶ What level of independent assurance am I willing to offer my customers?

“In most jurisdictions, the CSP itself is likely ultimately responsible for reporting and remitting indirect taxes such as sales and use taxes, even if an agreement states that it is the responsibility of the cloud user. Taxpayers are advised to carefully understand the rules and requirements and to ensure the appropriate processes are in place at the outset.”

Drew Alltizer
Tax



Similarly, outside the US, certain nations subject services to value-added tax (VAT), goods and services tax (GST) – or other forms of indirect taxation.

Once a CSP has determined revenue characterization, the CSP must determine where it has a taxable presence or nexus for both income and sales or use taxes so as to properly comply with regulations in the appropriate jurisdictions. Nexus determination not only governs taxation and the amount thereof, but can also determine whether filings are required (irrespective of whether any tax is due). In the current environment, CSP multinationals are often surprised by the potential nexus questions and answers that arise in establishing current business models. This is especially true with respect to non-US multinationals operating virtually in the US as well as US multinationals operating in large organized economic communities such as the EU.

There is, however, one positive element for CSPs in today's environment: since cloud services are often provided via a network of local data centers, and many localities offer constantly changing special tax and other cash incentives, careful planning can create

competitive advantage for CSPs as they seek to build out data centers in the US and abroad. "Many different jurisdictions are eager for economic development, so they will offer abatements or holidays for sales tax or VAT or even reduced rates of overall income taxation based on profits derived from activities based in their jurisdictions," explains Drew. Current technology requires that CSPs rely on physical substance somewhere, so consideration of the jurisdiction(s) in which to locate this activity is paramount, including whether tax incentives may factor into the overall business decision as to where to locate the data centers.

Transfer pricing (generally defined as the intra-company allocation among various jurisdictions/entities of the overall profit elements within related-party transactions) is another key issue to consider in designing or subscribing to a CSP arrangement. Taxpayers are advised to consider and clearly identify where the risk and value functions exist in CSP arrangements to ensure that each jurisdiction's profits are determined and reported on an arm's-length basis (determined as if the intra-company entities were unrelated).

"Many cloud computing service arrangements are technological evolutions of existing online/internet service and software delivery models. Accessing the insight of an experienced advisor in this area is helpful to understand the complex rules and the issues involved, as well as the uncertainties and overall tax planning opportunities."

Channing Flynn
 Global Technology Industry
 Tax Services Leader



CSPs and overall service company arrangements

Many of the world's countries have entered into income tax or other related tax treaties that may govern certain elements of the tax profile for CSPs operating in cross-border arrangements including withholding tax or nexus determinations. Tax treaties are generally designed to offer tax savings or more relaxed rules for the signing parties; CSP multinationals should ensure that they understand the tax treaty implications of their contemplated arrangements and comply with requisite compliance elements for obtaining benefits of various tax treaties.

Such issues will become an increasing concern for global multinational companies in all industries. As multinationals respond to their customers' requests for global service delivery, cloud computing models will play a critical role in how these companies build their service delivery models. Amy Ritchie, International Tax and Americas Tax Technology Leader says, "As multinational companies design service level models and consider how to move people and data to provide 24/7 service delivery in all time zones, consideration of cloud models is key. There is significant need among US multinationals to understand the complexities and opportunities inherent within global service delivery models, including how cloud arrangements are integrated within them."

Ernst & Young observations

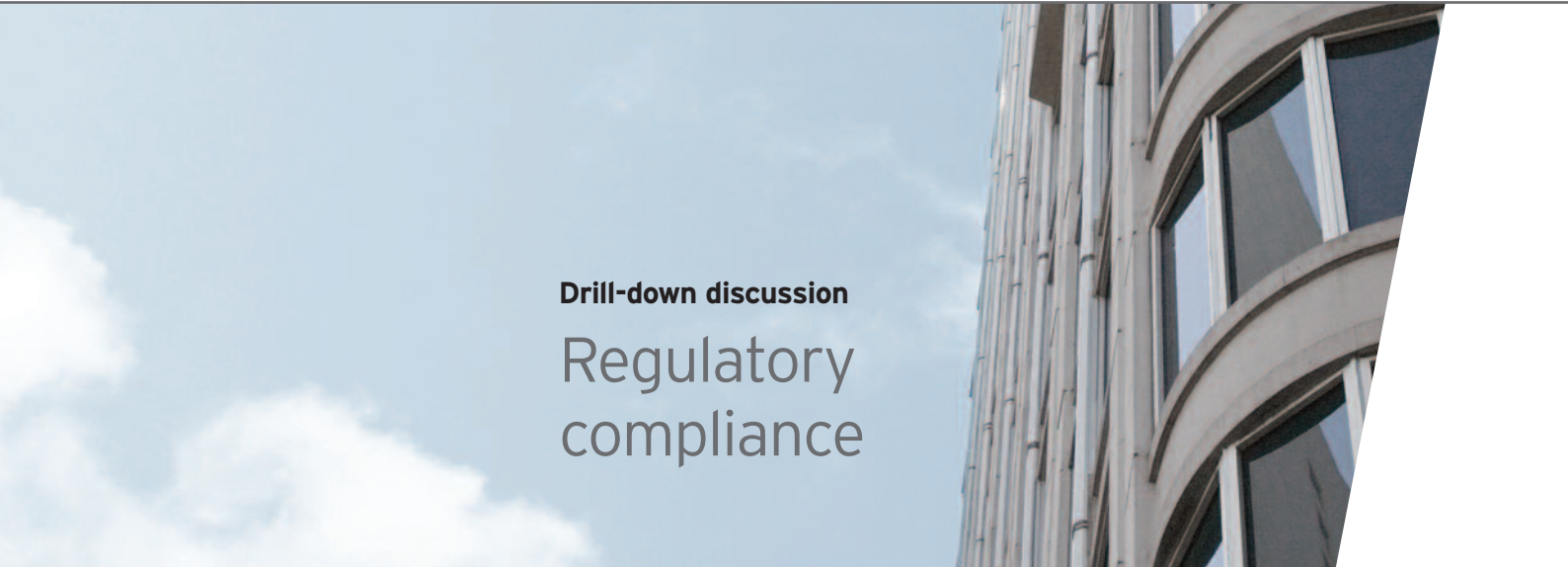
Analyzing the underlying substance of the CSP's product offerings and customer contracts will assist appropriate revenue characterization.

Determining where and whether a CSP has a taxable presence is a necessary step in designing new business models or subscribing to a CSP offering.

The full range of tax implications for CSPs will continue to evolve.

CSPs should approach CSP design and tax compliance as a potential competitive advantage. One way to achieve this is through assurances on design models that help cloud users maintain compliance with all tax regulations in the jurisdiction in which they operate.





Drill-down discussion

Regulatory compliance

More than half (52%) of North American and European business IT decision-makers said they were concerned or very concerned about regulatory compliance.¹

Current situation

Over the course of history, nations have evolved complex regulatory frameworks emerging out of their own distinct circumstances and cultures, and organizations that operate globally work to comply with all of them. Cloud computing services, meanwhile, often strive to be borderless in order to optimize the productivity of their infrastructures. When global organizations deploy cloud services, potentially material compliance issues arise for users of cloud services – and potential opportunities for CSPs.

With regard to compliance issues, some CSPs provide limited or no transparency about where data is being processed and stored within their network (the “global cloud” approach). More often, however, cloud service is provided by a group of interrelated but distinguishable data centers in different locations (the “network” approach). Cloud users may be subject to all or some of the compliance regulations in all the jurisdictions through which the cloud network passes. The key issues for cloud users are determining which compliance regulations need to be addressed as a result of where a CSP’s data centers are located, and the level of support their CSP provides in meeting those compliance requirements.

Cloud compliance considerations

Using a CSP means inviting another party to all of your business' regulatory compliance activities, ranging from tax requirements to internal controls policies to privacy statutes, industry-specific requirements and other legal considerations. This can complicate compliance activities or, if a CSP is strategic, enhance them. Cloud users have ultimate compliance responsibility – they are the ones who must determine how to capitalize on the benefits of cloud computing, while adhering to compliance requirements. In a recent study of North American and European enterprise and small to medium business (SMB) IT decision-makers, more than half are very concerned with the monitoring and auditing, regulatory compliance, overall internal controls and data protection capabilities of CSPs.²

The nature of the cloud complicates compliance issues

IaaS and PaaS vendors typically use a network approach, which potentially opens their users up to compliance regulations in each of the jurisdictions in which the CSP operates. While this expansion of compliance could be a bit overwhelming,

the alternative of a true global cloud means that you likely have that same expansion, but the nature of the cloud precludes you from knowing exactly where the issues exist.

For example, a cloud user may be subject to privacy laws, like the USA Patriot Act and EU Data Privacy Initiative based on the locations of its CSP's data centers. These and other privacy regulations limit what can and cannot be done with information, especially as it relates to moving across borders. "It is often unclear to the user where the information will be and where will it travel and therefore how they need to address regulatory requirements," explains Sagi Leizerov, Advisory – IT.

As a result of these considerations, compliance issues are likely to influence the types of applications and business processes that are candidates for cloud deployment, as opposed to traditional outsourcing. As compliance issues are addressed or resolved, strategic sourcing opportunities determined to be unfeasible today may become feasible tomorrow, depending on how the market evolves.

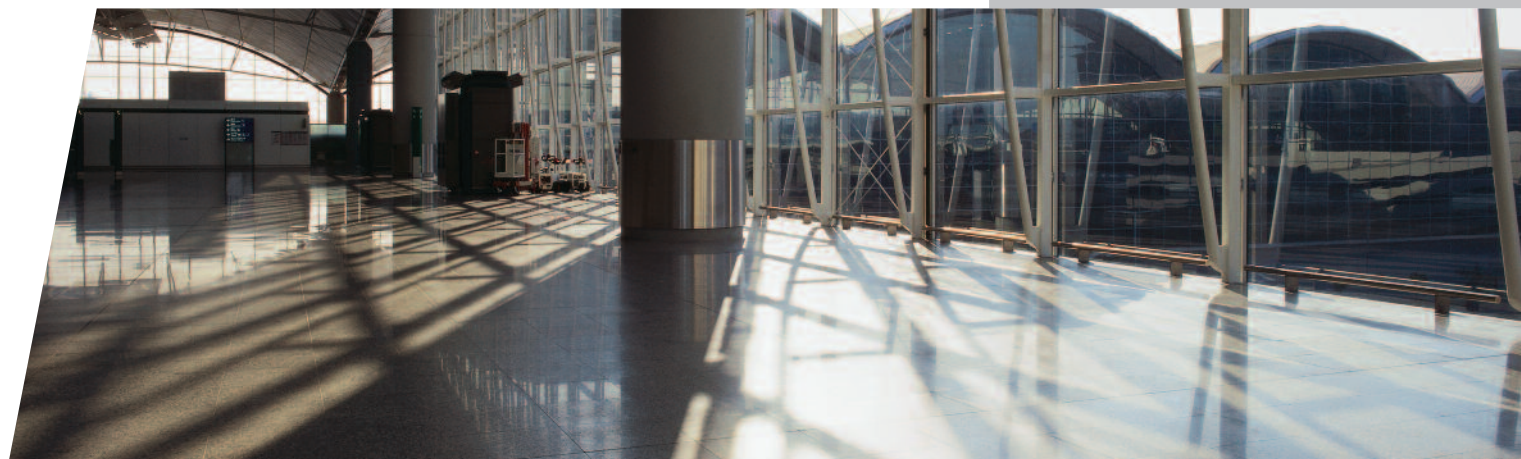
Questions to consider

Cloud business user

- Have I adequately considered compliance issues in the selection of my CSP, and are they clearly documented in our agreement?
- How will I monitor CSP adherence to agreed-upon compliance duties?
- How will the relationship with my CSP adapt to changing regulatory requirements?
- Should I consider moving to a community cloud, where all tenants share common compliance goals, instead of a fully public cloud?
- Have I considered working with a cloud broker?

Cloud service provider

- What level of independent assurance of compliance with local and regional jurisdictions' regulations am I willing to offer my customers?
- Is there an opportunity for competitive advantage by offering guaranteed compliance with specific government or industry regulations?





Cloud computing

is often borderless, but regulatory compliance is not

Industry-specific compliance issues

Other key compliance regulations that may require special arrangements between cloud users and their CSPs are the Payment Card Industry Data Security Standards (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA) in the US, and the Data Privacy Directives in the EU. Unfortunately, CSPs generally avoid customization because it isn't economically feasible. However, some predict the creation of specialized "compliant clouds" that will offer certified compliance with specific regulations for different industries, including a guarantee to store and manage data within the borders of a given nation, as appropriate.³

Importantly, such specialization is likely to come with a price. Compliance requirements imposed by governments or industries that restrict where data and processing

can physically occur tend to complicate all cloud business models by creating obstacles to optimal infrastructure utilization. To accommodate these challenges, CSPs are likely to develop pricing models with multiple tiers for different service levels that relate to customers' compliance requirements. For example, factoring strict compliance with the laws of multiple national jurisdictions into a service would cause that service to be priced higher than the same service without any compliance strictures.

E-discovery is another important area of compliance. "When data is spread in multiple locations at a CSP and a cloud user is served with a court order to produce data within a certain time period, how do they access it? Is it potentially comingled with other tenants' data?" asks Jose Granado, Advisory – IT.

“What are the assurances that you’re getting from the vendor that it has the proper controls in place, whether security and privacy controls, or controls that may be necessary to comply with all the regulatory issues?”

Alex Bender

Technology Industry – Assurance



Co-managing controls

In terms of controls, cloud users sometimes find controls that were previously managed internally are now being managed entirely by the CSP or are co-managed. Evaluating how the CSP manages controls becomes critically important for compliance with various regulations, such as the Sarbanes-Oxley Act in the US. Such evaluations are challenging enough in private cloud scenarios and far more so when public cloud services are used.

Intermediaries may provide compliance solutions

The rise of cloud brokers as intermediaries between service providers and business users may assist cloud users with compliance issues. Cloud brokers generally assist businesses with CSP selection, intermediation (such as building additional security or management layers) and aggregation when deploying customer services over multiple clouds. Cloud brokers also can provide a central point of governance and compliance expertise.⁴ Use of a community cloud – a cloud service shared by organizations with similar compliance or other concerns – is another way to mitigate compliance issues.

Ernst & Young observations

CSPs should approach compliance as a potential competitive advantage. One way to achieve this is through assurances that help cloud users maintain compliance with all regulations appropriate to the market in which the CSP wishes to create advantage.

Cloud users should do their due diligence, especially if they deal with regulated data, to determine what contractual commitments and what technical capabilities, processes and procedural support a CSP offers – and how they can be monitored.



Outlook

As the vision of IT delivered with the same reliability, flexibility and scalability as a public utility service takes hold, the implications are enormous for businesses and consumers worldwide. Despite lingering concerns about security, privacy and regulatory, legal and compliance issues, as well as the fundamental need to transform existing corporate and IT cultures, we believe the success of cloud computing is inevitable, because companies will be attracted to its flexible, pay-as-you-use business model. That model allows companies to manage their technology costs more efficiently, enables deployment of new technology faster and easier than other models, and allows management to focus on delivering business value.

“As the cloud gains traction in the marketplace, its potential to transform the business enterprise will become truly remarkable.

The corporation will undergo dramatic changes to infrastructure, processes and talent as it shifts to identifying and investing in opportunities and managing complex supply chains in the clouds.”

Paul van Kessel
Advisory – IT

As the cloud computing model becomes mainstream, higher-level services, which we call business process as a service, will evolve. Today, CSPs create efficiency through scale and expertise, solving IT challenges once and selling the solution to multiple buyers. That, in turn, is enabling another business model to emerge as business service providers begin to create value similarly. They will be solving business process challenges once and selling their solutions to multiple buyers – and those solutions will be built atop a pyramid of multiple cloud-based IT services. Such services will become increasingly specialized to maintain competitive advantage and profitability. Service buyers will have to look beyond just the first tier of CSPs they interact with to get visibility into risks and the assurance that these risks are being well-managed.

The current shift to cloud computing will enable organizations to finally achieve real business agility with regard to IT, enabling far more nimble responses to rapid market changes than are possible based on in-house IT. A future shift to cloud business processes would enhance that agility further, leading to far more remarkable potential to transform enterprises.

This vision has been discussed for a decade or more. At the 2001 World Economic Forum in Davos, similar thinking was envisioned as causing a transformation profound enough to be referred to as the death of the modern corporation.¹ That Davos meeting, however, took place a month before the dot-com crash that began in March 2001, which dashed such lofty rhetoric – for a time. Today, the advent of cloud computing has provided clarity about how such transformations might happen and the business models that might enable them.

For one thing, talk of corporations “dying” seems melodramatic today. Instead, corporations are likely to be transformed over time into a “conductor” of business – orchestrating the functions of a loose federation of service providers (which of course are themselves corporations) that come together in the cloud to deliver holistic, one-stop-shop solutions. In the coming years, the corporation will undergo dramatic changes to accommodate the future – changes to infrastructure, processes and talent as it shifts to a focus on identifying and investing in opportunities and managing complex supply chains and other outsourced providers in the cloud.

As businesses gain agility through cloud computing and business process as a service, consumers will gain unprecedented access to information. Both come about through the innovative “mashing up” of multiple services – i.e., combining existing services in new and innovative ways to create new business value, whether through open application programming interfaces or via private service contracts. In an April 2010 speech at the Brookings Institution, US CIO Vivek Kundra offered a compelling description of the business side of this vision:

“Cloud computing will give rise to virtual organizations. Unencumbered by the physical constraints of data centers, hosting providers and hardware platforms, these virtual organizations can focus solely on customer needs, tapping into the near limitless array of options the cloud will provide. In the same way we now create mash-ups to combine and analyze data from disparate websites, new companies will emerge that tie together services from vast networks of suppliers and customers to create a range of new and more agile products and solutions.”²

As this shift happens, organizations will need to develop new competencies to remain competitive. For example, they may need the ability to quickly establish and dissolve agreements and partnerships, suggesting legal and operations teams that can draw up contracts quickly that are favorable to all partners in a chain. And they may need improved ability to manage partner relationships involving cross-company business processes, to take advantage of the dynamic provider marketplace that is envisioned.

We see this vision as a large opportunity for companies to create value by bringing together multiple pieces, leading to a dramatic change in the way businesses and consumers access information and, therefore, in the way we see the world around us. “For example, companies will be able to combine location data, map data, social networking data and business information, and serve them all up in a contextually relevant way,” says Paul Chabot, Global Technology Industry, Advisory – PI.

“Through a mobile device like my phone, cloud applications can know where I am as I’m walking down the street,” says Paul. “With augmented reality applications, I could scan the horizon through my mobile phone’s camera and see information overlaid on the image of my surroundings. What businesses are located in the building I’m walking past? Is a store having a sale on my favorite designer? Is one of my friends there? Or, I can point my phone at someone passing by. The cloud does the image recognition and pulls all the information from their Facebook profile and shares with me who that person is. We’re getting to the point where that’s possible.”

Companies that are able to leverage cloud computing and business process as a service to pull together such mash-ups have the potential to unlock significant value in the not-too-distant future.

“Given the government’s ‘Kasumigaseki Cloud’ initiative, cloud computing is likely to stimulate new growth throughout the Japanese economy. Beyond the benefits of flexibility and scalability, it is viewed as a viable means to reduce energy consumption through efficient information management.”

Yuichiro Munakata
Japan Technology Industry Leader



Glossary of terms

Application service provider (ASP) is a term used to describe computer-based services delivered over the internet in the late 1990s. The term has since been replaced by “on-demand software” and “software as a service.”

Cloud computing¹ is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of (A) five essential cloud characteristics, (B) three service models and (C) four deployment models.

A: Essential cloud computing characteristics

1. *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
2. *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, PDAs).
3. *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, data center). Examples of resources include storage, processing, memory, network bandwidth and virtual machines.
4. *Rapid elasticity.* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
5. *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilized service.



B: Cloud computing service models

1. *Cloud software as a service (SaaS)*.

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. *Cloud platform as a service (PaaS)*.

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.

3. *Cloud infrastructure as a service (IaaS)*.

The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

C: Cloud computing deployment models

1. *Private cloud*. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

2. *Community cloud*. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

3. *Public cloud*. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

4. *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Grid computing is a form of distributed computing in which a large set of geographically remote computers work together to perform a single task. Although it started out as a more general term, today it applies primarily to supercomputer-level tasks and is used mostly in the scientific community.

Mash-ups are new, innovative combinations of existing services, usually on the internet, that create new business value, whether through open public means or via service agreements.

Time-sharing is the process in which multiple users share the processor time of a mainframe computer system. It faded out of use beginning in the 1980s after the PC emerged.

Utility computing is the provision of computing resources as a metered service, similar to a public utility. The term is an ancestor of cloud computing; it was most popular in the 1980s and early 1990s.

Service level agreements (SLAs) are written contracts between IT service providers and their customers that stipulate details such as system availability and customer service response time, as well as penalties for failure to meet the agreed-upon service levels.





Source notes

Opening statement

- ¹ "Enterprise cloud-based services market to treble by 2015," *Telecompaper World*, 23 July 2010, via Dow Jones Factiva, © 2010 Telecompaper.
- ² "Cloud Services To Top \$68 Billion In 2010," *CMP TechWeb*, 22 June 2010, via Dow Jones Factiva, © 2010 United Business Media LLC.
- ³ *IDC Predictions 2011: Welcome to the New Mainstream*, International Data Corporation, December 2010.
- ⁴ Ibid.

Overview

- ¹ *IDC Predictions 2011: Welcome to the New Mainstream*, International Data Corporation, December 2010.
- ² "Indie App Stores Struggle," *The Wall Street Journal*, 24 November 2010, via Dow Jones Factiva, © 2010 Dow Jones & Company, Inc.
- ³ "Cloud Security To Reap \$1.5 Billion By 2015," *InformationWeek.com*, 22 October 2010, via Dow Jones Factiva, © 2010 United Business Media LLC.
- ⁴ *IDC Predictions 2011: Welcome to the New Mainstream*, International Data Corporation, December 2010.
- ⁵ *Borderless Security: Ernst & Young's 2010 Global Information Security Survey*, Ernst & Young, 2010.
- ⁶ "The future for IT looks cloudy, with silver linings," *The Age*, 17 November 2010, via Dow Jones Factiva, © 2010 John Fairfax Holdings Limited.
- ⁷ "Information Age: Egypt's Revolution by Social Media," *The Wall Street Journal*, 14 February 2011, © 2011 Dow Jones & Company, Inc.
- ⁸ "Cloud Computing Gains Momentum but Security and Privacy Issues Persist," *DigitalCommunities.com*, 25 September 2009.

Pricing and business models

- ¹ "Evolution of the Cloud, Part 1 SAAS," *PluGGd in (India)*, 6 January 2011, via Dow Jones Factiva, © 2011 HT Media Limited; "Amazon Web Services slashes support pricing," *VNUNet United Kingdom*, 7 January 2011, via Dow Jones Factiva, © 2011 VNU Business Publications.

Vendor management and strategic sourcing

- ¹ David Mitchell Smith, "Hype Cycle for Cloud Computing, 2010," *Gartner, Inc.*, 27 July 2010.
- ² "Cloud Engineering: The CIO's Dilemma," *CIO Insight*, 20 July 2010, via Dow Jones Factiva, © 2010 Ziff Davis Enterprise Holdings Inc.

Availability and interoperability

- ¹ "Compliance With Clouds: Caveat Emptor," *Forrester Research Inc.*, August 26, 2010.
- ² "The Future of Cloud Computing: Opportunities For European Cloud Computing Beyond 2010," *European Commission*, 27 January 2010.
- ³ "Symbian Pledges Support for the Open Cloud Manifesto," *eWeek*, 2 July 2010, via Dow Jones Factiva, © 2010 Ziff Davis Enterprise Holdings Inc.
- ⁴ "IT user super group forces vendors to take notice; Open Data Center Alliance focuses on interoperability," *Network World Fusion*, 23 November 2010, via Dow Jones Factiva, © Network World, Inc.

Security and privacy

- ¹ "Cloud Security to reap \$1.5 Billion by 2015," *CMP TechWeb*, 22 October 2010, via Dow Jones Factiva, © 2010 United Business Media LLC.
- ² "IBM Introduces Security Services to Protect Cloud Environments," *eWeek*, 22 October 2010, via Dow Jones Factiva, © 2010 Ziff Davis Enterprise Holdings Inc.
- ³ "The Future of Cloud Computing: Opportunities For European Cloud Computing Beyond 2010," *European Commission*, 27 January 2010.
- ⁴ "Cloud Security to reap \$1.5 Billion by 2015," *CMP TechWeb*, 22 October 2010, via Dow Jones Factiva, © 2010 United Business Media LLC.
- ⁵ "Cloud Computing: 5 Things No One Will Tell You," *Biz-Tech 3.0*, 19 October 2010.
- ⁶ Cloud Security Alliance Official website, <http://www.cloudsecurityalliance.org>, accessed 8 October 2010.
- ⁷ *Proposed Security Assessment and Authorization for U.S. Government Cloud Computing, Draft Version 0.96*, 2 November 2010, accessed from cio.gov on 10 November 2010, <http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-edRAMP>.
- ⁸ "Microsoft Wins U.S. Agency Deal," *The Wall Street Journal*, 9 December 2010, via Dow Jones Factiva, © 2010 Dow Jones & Company, Inc.
- ⁹ "GSA Picks Google Email," *The Wall Street Journal*, 2 December 2010, via Dow Jones Factiva, © 2010 Dow Jones & Company, Inc.
- ¹⁰ *Borderless Security: Ernst & Young's 2010 Global Information Security Survey*, Ernst & Young, 2010.

- ¹¹ "Federal Agencies Could Save Billions by Switching to the Cloud; RightNow 'Safe Switch' Helps Federal Government Meet Stringent Certification and Accreditation to Move into RightNow's Secure Cloud Today," Business Wire, 13 April 2010, via Dow Jones Factiva, © 2010 Business Wire.
- ¹² "The legal considerations of cloud computing," *Computer Weekly*, 14 December 2010, via Dow Jones Factiva, © 2010 Reed Business Information Limited.

Standards and risk management

- ¹ "ERM & Internal Controls: Study Finds Gap in Privacy Expectations, Delivery," *Compliance Week*, 31 July 2010, via Dow Jones Factiva, © 2010 Haymarket Media.
- ² "Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security OJ C 321, 29.12.2009, p. 1-4," EUR-Lex, 7 January 2010, via Dow Jones Factiva, © 2010 European Communities.
- ³ "Feds Advance Cloud Adoption Plans," CMP TechWeb, 21 May 2010, via Dow Jones Factiva, © 2010 United Business Media LLC.
- ⁴ *Overview: NIST Cloud Computing Efforts, Proceedings of the NIST Cloud Computing Forum & Workshop*, 20 May 2010.
- ⁵ "House Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement Hearing – 'Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud,'" Congressional Documents and Publications, 1 July 2010, via Dow Jones Factiva, © 2010 Federal Information & News Dispatch, Inc.
- ⁶ Distributed Management Task Force website, <http://www.dmtf.org/about>, accessed 10 November 2010.
- ⁷ "Cloud, smart computing to drive tech sector growth," Forrester, 16 December 2010, Business Line (The Hindu), via Dow Jones Factiva, © 2010 The Hindu Business Line.
- ⁸ "Groups Seek Cloud Computing Standards," CMP TechWeb, 15 July 2009, via Dow Jones Factiva, © 2009 United Business Media LLC.
- ⁹ Open Cloud Consortium website, <http://opencloudconsortium.org>, accessed 10 November 2010.
- ¹⁰ "SAS 70 is the measure of cloud security," Network WorldFusion, 23 June 2009, via Dow Jones Factiva, © 2009 Network World, Inc.
- ¹¹ "Cloud, smart computing to drive tech sector growth," Forrester, 16 December 2010, Business Line (The Hindu), via Dow Jones Factiva, © 2010 The Hindu Business Line.

Government

- ¹ "Federal CIO Views Cloud Computing As Safe, Economical, And Efficient," IP Network Policy Report, 12 April 2010, via Dow Jones Factiva, © 2010 Aspen Publishers.
- ² Ibid.
- ³ "Government Closer to Universal Cloud-Computing Security Assessment and Authorization Program," Targeted News Service, 2 November 2010, © 2010 Targeted News Service.
- ⁴ "Microsoft Wins U.S. Agency Deal," *The Wall Street Journal*, 9 December 2010, via Dow Jones Factiva, © 2010 Dow Jones & Company, Inc.
- ⁵ "GSA Picks Google Email," *The Wall Street Journal*, 2 December 2010, via Dow Jones Factiva, © 2010 Dow Jones & Company, Inc.
- ⁶ "The Future of Cloud Computing: Opportunities For European Cloud Computing Beyond 2010," European Commission, 27 January 2010.
- ⁷ "Building Britain's Digital Future; Government Unveils Action Plan for the Digital Economy; Digital Economy central to industrial strength and competitiveness; Communications Infrastructure critical for future economic growth," M2 Presswire, 16 June 2009, via Dow Jones Factiva, © 2009 M2 Communications, Ltd.
- ⁸ "Japan Hopes IT Investment, Private Cloud Will Spur Economic Recovery," CMP TechWeb, 15 May 2009, via Dow Jones Factiva, © 2009 United Business Media LLC.
- ⁹ "Shanghai to invest in cloud computing," *Shanghai Daily*, 27 October 2010, via Dow Jones Factiva, © 2010 Shanghai Daily Company.
- ¹⁰ "China to develop cloud computing services in five pilot cities," Interfax: China Telecom Newswire, 22 October 2010, via Dow Jones Factiva, © 2010 Interfax Information Services B.V.
- ¹¹ "One on One: Vivek Kundra, U.S. Chief Information Officer," NYT Blogs, 5 November 2010, via Dow Jones Factiva, © 2010 The New York Times Company.
- ¹² Cloud Computing, keynote presentation by Ira A. (Gus) Hunt, Chief Technology Officer, CIA, for the Virtualization, Cloud Computing and Green IT Summit, 27 October 2010.
- ¹³ "Federal Agencies Could Save Billions by Switching to the Cloud; RightNow 'Safe Switch' Helps Federal Government Meet Stringent Certification and Accreditation to Move into RightNow's Secure Cloud Today," Business Wire, 13 April 2010, via Dow Jones Factiva, © 2010 Business Wire.

Accounting

- ¹ *Worldwide and Regional Public IT Cloud Services, 2010-2014 Forecast*, IDC, June 2010.
- ² *IFRS Outlook, Insights on international GAAP*, Ernst & Young, July 2010.

Cross-border taxation of CSP arrangements

- ¹ "The states strike back; Aim to boost revenue with tough new sales and use tax strategies," *Accounting Today*, 13 September 2010, via Dow Jones Factiva, © 2010 Accounting Today and SourceMedia, Inc.

Regulatory compliance

- ¹ Enterprise And SMB Security Survey, North America And Europe, Q3 2009, Forrester Research.
- ² Ibid.
- ³ Source: IDC Predictions 2011: Welcome to the New Mainstream, International Data Corporation, December 2010.
- ⁴ "Layer 7 Technologies; Layer 7 Launches New Cloud Security, Connectivity and Management Solutions," *Telecommunications Weekly*, 5 May 2010, © 2010 Telecommunications Weekly via NewsRx.com

Outlook

- ¹ "Davos economic summit and globalization – yet another spate of opposition," *The Independent*, 5 February 2001, via Dow Jones Factiva, © 2001 Knight-Ridder/Tribune Business News.
- ² "One on One: Vivek Kundra, U.S. Chief Information Officer," NYT Blogs, 5 November 2010, via Dow Jones Factiva, © 2010 The New York Times Company.

Glossary of terms

- ¹ The definition of cloud computing and its essential characteristics, service models and deployment models is excerpted from the US National Institute of Standards and Technology's widely referenced definition, NIST Definition of Cloud Computing v15. The full text is available at the NIST web site at <http://csrc.nist.gov/groups/SNS/cloud-computing/>

Ernst & Young's Global Technology Center contacts

Pat Hyek

Global Technology Industry Leader
pat.hyek@ey.com
+1 408 947 5608

Yuichiro Munakata

Japan Technology Industry Leader
munakata-ychr@shinnihon.or.jp
+81 3 3503 1528

Rebecca Norris

EMEIA Technology Industry Leader
rnorris@uk.ey.com
+44 1189 28 1140

Joe Tsang

Asia-Pacific Technology Industry Leader
joe.tsang@cn.ey.com
+86 10 5815 2902

Channing Flynn

Global Technology Industry Tax Services Leader
channing.flynn@ey.com
+1 408 947 5435

Kevin Price

Global Technology Industry Advisory Services Leader
kevin.price@ey.com
+1 415 894 8229

Joe Steger

Global and Americas Technology Industry Transaction Advisory Services Leader
joseph.steger@ey.com
+1 408 947 5488

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

How the Ernst & Young Global Technology Center can help your business

The technology industry is in a constant state of change – driven by continuous innovation, shifting markets, converging industries, consumer demand and the need for first-mover advantage. Ernst & Young's Global Technology Center connects a worldwide team of more than 14,000 technology professionals to help you navigate the challenges of this continuous change. We provide assurance and tax guidance through a network of experienced advisors to help you manage risk, transform business performance and sustain improvement. We can help you deliver cost-effective innovation, balance product portfolios, maintain effective supply chains, and identify, execute and integrate strategic growth transactions. Our global technology network leverages our leading market share position in serving technology companies to provide you with timely, reliable information. Our teams use a cross-discipline, collaborative approach to help you achieve your business objectives. We encourage our people to use their ingenuity and initiative to help you develop approaches, create options and seize opportunities. It's how Ernst & Young makes a difference. www.ey.com/technology.

© 2011 EYGM Limited.
All Rights Reserved.



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

EYG No. DC0078