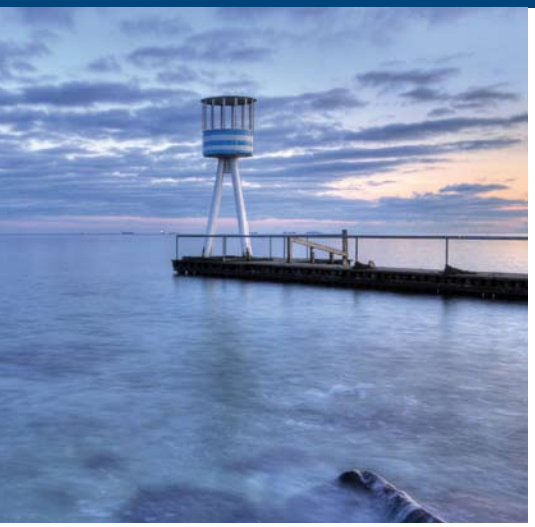

Assurance in the cloud

The impact of cloud computing on financial statements

M. Chung
is a manager at KPMG Advisory. He is primarily concerned with issues concerning cloud computing, outsourcing and online services. Mike is a frequent speaker at conferences and seminars, and regularly publishes on IT topics in a variety of journals.

chung.mike@kpmg.nl

Mike Chung

Cloud computing seems likely to outgrow the hype stage in 2011. There is a growing realization that cloud computing has a far-reaching impact on the degree of assurance provided by financial statements, in particular concerning annual reports and accounts. Cloud computing means external data storage on the cloud provider's premises, the sharing of IT resources and dependency upon the public internet. Therefore, the steadily progressive shift from locally installed and maintained IT to the cloud makes it necessary for potential customers to be adequately informed about the following key issues: What is cloud computing? How does cloud computing impact the degree of assurance, in particular concerning financial statements? What steps should be taken? This article will provide answers to these questions.

Introduction

Cloud computing is undoubtedly the most significant phenomenon in IT today. The provision of IT services via the internet, what cloud computing is essentially all about, seems likely to outgrow the hype stage in 2011. A recent study by KPMG shows that nearly 60 percent of Dutch companies are already using cloud services for one or more parts of their IT, or intend to switch to cloud solutions within the next 12 months. The same study also indicates that the majority of respondents consider cloud computing to be the future model of IT. However, it should be noted that of the total expenditures on IT at these companies, the share allocated to cloud computing is still marginal (less than 5 percent) ([KPMG10]).

While the established pioneers of cloud computing (Salesforce.com, Amazon and Google being the best known) are steadily expanding their service portfolio, almost all major IT providers are investing heavily in cloud services in order to meet the apparently rising demand. Microsoft, IBM and Oracle are all offering cloud services and cloud-enabling technology to facilitate business processes, occasionally in collaboration with other software companies and IT integrators.

Amidst the cloud euphoria fanned by IT providers and "independent" analysts, there is a growing realization that cloud computing has a far-reaching impact on the degree of assurance provided by financial statements, in particular concerning annual reports and accounts. Factors of importance to financial business processes (access control and authorization,

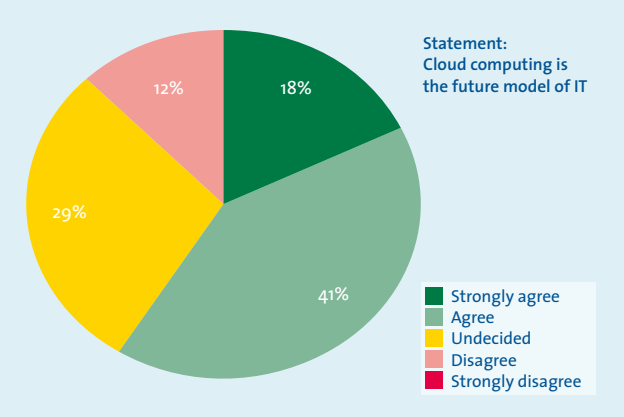

Figure 1: **Statement based on responses of 125 decision-makers** ([KPMG10])

change management, backup and recovery) have different risk profiles in the cloud than they have when they are part of traditional, on-premise systems. As a rule, and from the viewpoint of the customer, cloud computing means external data storage on the cloud provider's premises, the sharing of IT resources and dependency upon the public internet.

Therefore, the steadily progressive shift from locally installed and maintained IT (also known as on-premise IT) to the cloud makes it necessary for potential customers to be adequately informed. For them, information about the following key issues is important:

- What is cloud computing?
- How does cloud computing impact the degree of assurance, in particular concerning financial statements?
- What steps should be taken?

This article will provide answers to these questions.

What is cloud computing?

Definition

A search using Google or Bing delivers a multitude of definitions, descriptions and opinions on cloud computing. Some speak of "applications on the internet" or "computational style in which IT provides scalable and flexible capabilities as services to external customers through the use of internet technology," while others qualify it with terms such as "old wine in new bottles." Obviously, there is a lack of consensus and a lot of confusion on what cloud computing actually is.

Simply stated, cloud computing means the provision of IT services from shared resources via the internet. The internet is often metaphorically depicted as a cloud, hence the term cloud computing. Well-known examples of cloud computing are Gmail, Google Apps, Hotmail and Apple's MobileMe.

The reason why this seemingly simple concept is explained so differently by IT providers, analysts and academics is mainly due to the fact that cloud computing does not only involve technological but also important business elements. From a technological perspective, cloud computing is based upon already existing technologies such as virtualization, web services, shared data caches, and grid computing. Since ASPs (Application Service Providers) have been providing IT applications over the internet for more than a decade, cloud computing can indeed be denoted as "old wine in new bottles."

However, the commercial provision of IT services over the internet on a large scale from shared pools of IT resources has only become economically viable due to three relatively recent developments. Firstly, the above-mentioned technologies, of which virtualization and web services are the most important, have been refined, standardized and widely applied during the last five years. Secondly, public broadband networks have become abundant and readily available at reasonable cost. Thirdly, some providers have expanded the scale of their IT resources enormously, making them the major players in the cloud computing market of today.

The business principle of cloud computing is based on the fact that *possession/ownership* of IT resources (*i.e.* applications, platforms or infrastructure) is independent of *use* of these resources. In cloud computing, IT resources, whether it is an application or storage, remain the property of the cloud service provider; customers only pay for the use of the IT service without requiring local soft- or hardware installations. In theory, cloud computing does not require upfront investments (capital expenditures) unlike the traditional, on-premise IT. The customer only needs access to the internet.

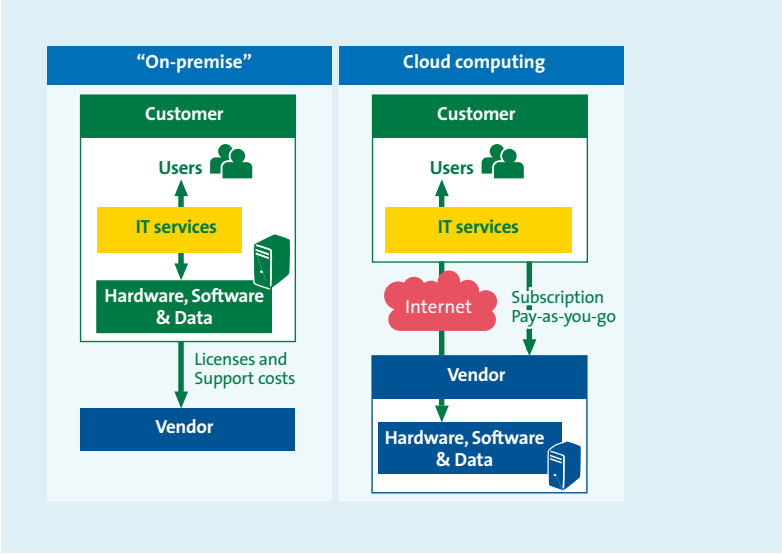

Figure 2: **On-premise IT versus cloud computing** ([KPMG10])

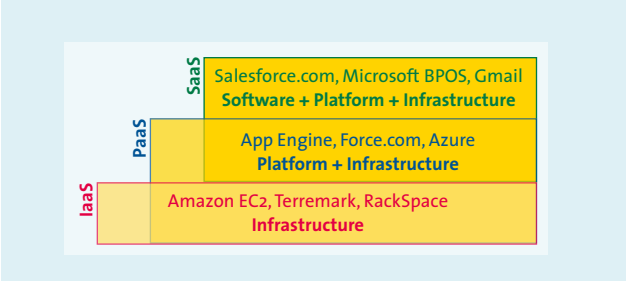

Figure 3: **Different layers of cloud computing** ([KPMG10])

Layers, characteristics, and types

Cloud services can be offered at various layers of IT. At the software layer, such a service is called Software-as-a-Service (SaaS). Platform-as-a-Service (PaaS) provides IT services at the platform level (*e.g.* operating systems, application frameworks); in this case, additional software must then be developed or installed by customers. Infrastructure-as-a-Service (IaaS) provides technical infrastructure components (*e.g.* storage, memory, CPU, network). Additional platform elements and software have to be installed by the customer, or specific infrastructure components can be utilized for on-premise processes (see Figure 3). Generally, cloud service providers specialize in one or two layers only.

Depending on the layer, cloud computing has the following characteristics:

- *External data storage and processing.* Unlike on-premise IT, data is stored and processed outside the customer's domain at the cloud service provider's location(s).
- *Multi-tenancy.* Contrary to on-premise IT, resources are shared, to a certain degree, by multiple customers.
- *Internet dependency.* Although leased lines and proprietary networks can be used for cloud computing, the primary infrastructure of cloud computing is the public internet.
- *Contracted services.* Customers pay for a service (pay-as-you-go or subscription) instead of licenses and/or hardware.
- *On-demand services.* In contrast to the vast majority of on-premise IT, cloud services can be used almost instantly.
- *Elasticity.* Cloud services can be easily upscaled and downsized.

Multi-tenancy may be limited to a select group of customers or even a single customer, although there is always a degree of multi-tenancy (*e.g.* physical facilities, cooling, supporting staff) with cloud computing. This form of private or dedicated cloud computing represents an alternative to the public cloud, which has a high degree of multi-tenancy. In either form, customer data is stored at the provider's location(s).

Some providers offer private cloud computing solutions in which an organization's internal IT department uses cloud computing technologies to create an "on-premise cloud." Since this internal form of cloud computing is fully dependent on internal, on-premise IT, it is highly questionable whether this type can truly be called cloud computing. Therefore, any such notion of an internal cloud will not be discussed in this article.

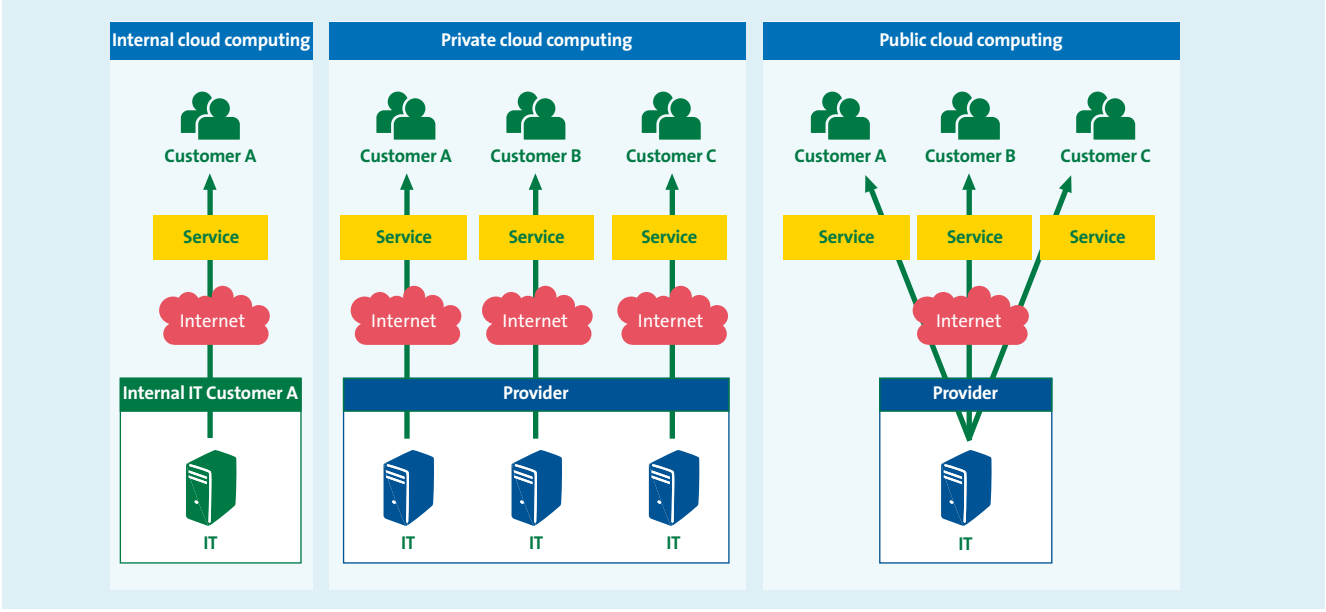

Figure 4: **Different types of cloud computing** ([KPMG10])

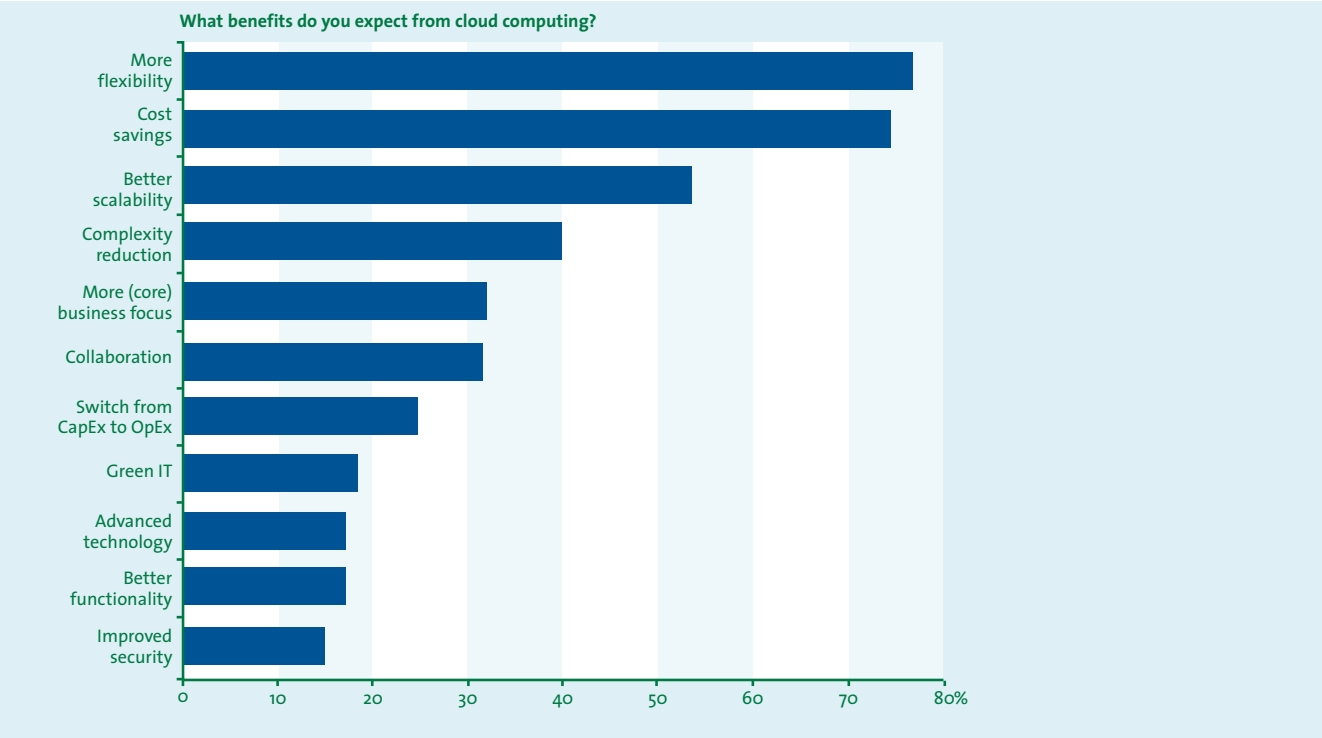

Figure 5: **Benefits of cloud computing based on responses of 125 decision makers** ([KPMG10])

Drivers of cloud computing

More flexibility

The success of cloud computing is partly due to the fact that the traditional, on-premise IT is increasingly being confronted with technical limitations and complexity while the costs of implementing and maintaining IT systems are scarcely kept under control. Outsourcing and offshoring have only partially solved the problems, and the promised cost savings rarely turned out to be achievable. Cloud computing seems to offer the ideal solution in this respect; it enables companies to phase parts of their IT, including hardware, software and IT personnel. Companies can regain authority over their business, required IT services are obtained over the internet, and the costs are transparent and relatively easy to control.

A recent survey by KPMG revealed that nearly 60 percent of cloud computing customers feel flexibility is the most important benefit. Cloud services can be purchased and used quickly since installation has already been done by the provider, including all associated requirements to manage the IT resources, construct physical facilities and provide security. This is in stark contrast to the lengthy and risky deployment projects that are so typical of on-premise IT ([KPMG10]).

Cloud computing also has the advantage of keeping software development and updates largely out of the customer's sight. Ideally, the customer only defines a set of specifications and requirements, according to which the provider implements the updates and changes on the relevant parts of the IT environment. The customer is only required to conduct functional tests and decide on acceptance. Consequently, annoying updates to IT systems are a thing of the past.

Cost-savings

IT operational costs can be reduced significantly by adopting cloud computing, since this model's initial investments (capital expenditures) are marginal compared to the costs that are involved with large-scale, costly and risky implementations of on-premise IT resources. All installations actually take place on the provider's servers, and the management costs for making the services continuously available are borne by the provider. Moreover, there are considerable savings in terms of hardware, server rooms, air conditioning and electricity. The costs passed on to customers are relatively low due to the economies of scale of most cloud service providers, efficient use of (shared) resources, and centralization of expertise.

With cloud computing, charges only apply to the use of the IT service, as the IT resource remains in the possession of the provider. Although subscriptions are still the rule, "pay-as-you-

go" has come into vogue recently, enabling the customer to pay each time the service is employed. The advantage of pay-as-you-go is that payment is only made for services that are actually used, and unnecessary overhead is avoided.

Still, it should be noted that, although the initial costs of cloud computing are significantly lower than on-premise IT, the costs of cloud computing remain constant throughout the life cycle of the relevant IT resource, supposing that demand remains constant. The costs of local facilities will, however, diminish gradually, due to depreciation. The cost-savings of cloud computing are therefore highly dependent on the duration of the product life cycle. The longer an IT resource is used, the lower the relative advantage of cloud computing in relation to on-premise IT.

Better scalability

Cloud computing also offers the advantage of being able to adjust the use of IT resources either upwards or downwards, thus improving the scalability of IT.

By using various types of virtualization and load-balancing, cloud computing solutions can easily be scaled up and down. Combined with the "pay-as-you-go" or subscription models that are common to cloud computing, customers only pay for what they use and the required IT capacity is always available (in theory). In contrast to on-premise IT, IT capacity is never idle and never scarce.

Into perspective

Notwithstanding the valid drivers of cloud computing and the hype, cloud computing should be put into perspective. The share of IT expenditures allocated to cloud computing is still marginal. Depending on the analysis, the share allocated to cloud computing as of 2010 is between 2 and 4 percent, with the US as the leading outlet of cloud services (60 percent); the rest of the world, including Europe, can be considered as peripheral. No matter how popular cloud computing is in our social lives (Facebook and Gmail as typical cloud services), large-scale adoption of cloud computing by the corporate community is yet to come. For the time being, at least until 2015, traditional, on-premise IT will be the dominant factor ([KPMG10], [OECD10]).

Yet, the emergence of cloud computing cannot be ignored: it is growing between 20 and 40 percent per year, despite (or perhaps thanks to) the economic low tide. Moreover, the move towards centralization and consolidation of IT resources and management is a process that has been taking place since the turn of the millennium. From locally installed IT, many companies chose to set up Shared Service Centers (SSH) in order to make more efficient use of their IT. Then came the waves of hosting applications on external platforms and infrastructure, and outsourcing/offshoring. In this respect, cloud computing can be seen as the next phase in this process and part of the paradigm shift in automation from locally installed/managed IT towards centralized delivery and shared use of services ([KPMG10], [OECD10]).

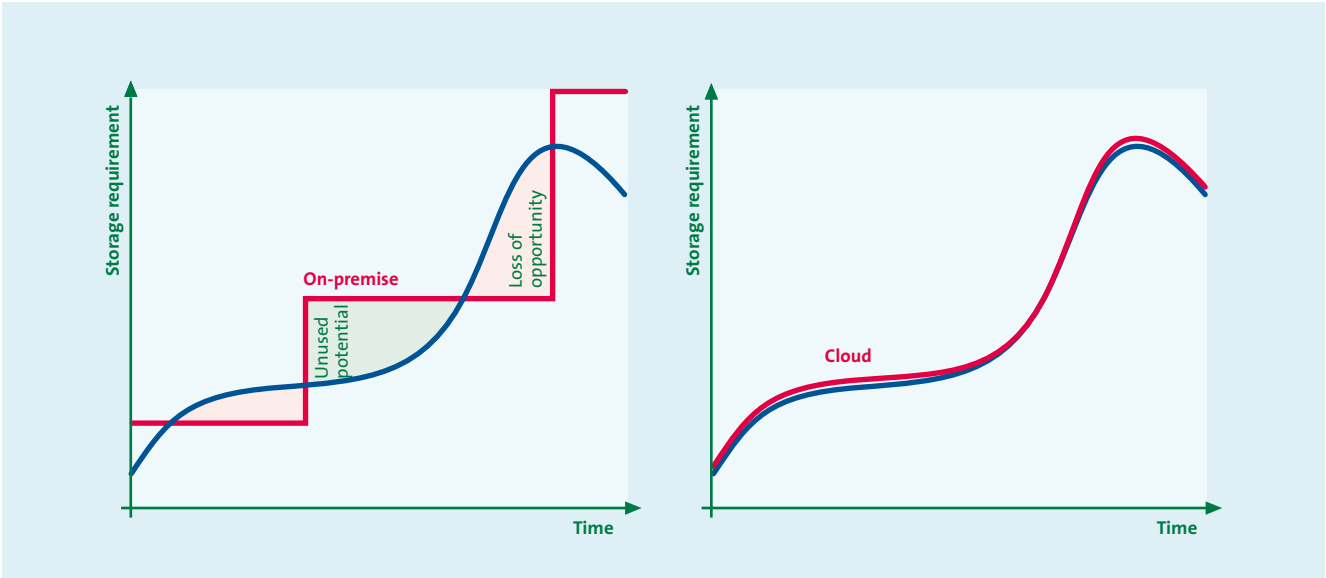

Figure 6: **Scalability of cloud computing** ([KPMG10])

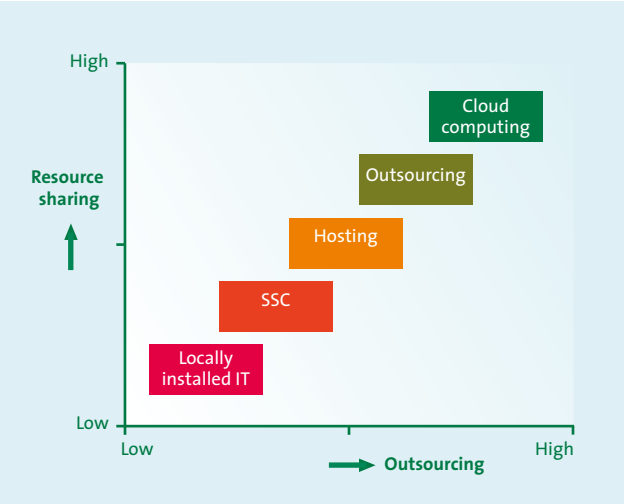

Figure 7: **Paradigm shift** ([KPMG10])

The impact of cloud computing on assurance

Relevant factors

The number of cloud services that are mature and proven is rather limited, although CRM, e-mail, "office" software, document sharing and storage as cloud services are gaining a stronghold in the market. Given this impressive pace of development and growth, even financial software services from the cloud will become common in the near future. As a matter of fact, SaaS for accounting purposes, such as Twinfield and NetSuite, have a well-established reputation amongst mid-sized companies. It will take a while before ERP at Fortune 500 companies will move to the cloud, but the rise and expansion of cloud services is imminent, thus increasingly relevant to the issue of assurance provided in financial statements.

	On-premise IT	Cloud computing
Location of data storage and IT assets	• Within the (internal) security domain of the customer's organization	• Outside the internal security domain of the customer's organization • Hosted/located at cloud service provider or distributed/scattered over a multitude of (third party) providers
Usage of (IT) resources	• Exclusive for the customer	• Various degrees of multi-tenancy
Primary infrastructure for data transfer	• LAN • Leased lines	• Public internet

Table 1: **Characteristics impacting risk profile**

When we focus on the specific impact of cloud computing on the degree of assurance, particularly in financial statements, the following factors must be taken into consideration:

- access control and authorization;
- change management; and
- backup and recovery.

Generally, these are the most important IT topics for investigation within the scope of financial audits.

Risk profile

Cloud computing is not devoid of dangers. Although the number of major incidents involving commonly used cloud services was relatively small in 2010 in relation to the number of customers, the foremost providers (Google, Salesforce.com, Amazon and Microsoft) have all had to remedy several critical vulnerabilities in their cloud offerings. Recently, weaknesses in Hotmail were exposed by hackers, who were able to obtain illegal access to thousands of accounts. Amazon's Elastic Cloud fell prey to Botnets, and leaks in Google's Web Service enabled unauthorized individuals to gain access to accounts and passwords.

Although these incidents were caused by various technical and process-related weaknesses, customer data stored at the cloud computing provider's location was, in all cases to a certain degree, compromised. All this emphasized at least one crucial point: the customer is strongly dependent on, if not entirely at the mercy of, the maturity of the cloud service provider.

The risks of cloud computing should be put into perspective. On the one hand, cloud computing is mainly based on existing technologies such as virtualization, data segregation and web services. So existing IT risks apply, albeit the controls and mitigating measures largely belong on the provider's side, as the provider owns and manages the IT resources in the cloud. On the other hand, cloud computing has characteristics that considerably affect the risk profile compared to the traditional, on-premise IT. These characteristics are:

- external data storage and processing;
- sharing of IT resources with other customers (multi-tenancy); and
- dependency on the public internet.

Access control & authorization

Concerning access control and authorization, all three characteristics related to the risk profile of cloud computing apply. The off-premise nature of the cloud means that the customer depends on the provider's technology, personnel and processes. Multi-tenancy requires

an advanced level of authentication, authorization, and separation of data instances. The public internet involves multiple access points from countless locations, which are exceptionally difficult to control.

In practice, customers are confronted by three issues:
1. divergent degrees and forms of authentication;
2. complexity of integrating control processes; and
3. technical complexity of integrating authentication mechanisms.

Almost all cloud services offer their own forms of authentication. They can range from a combination of account and password (2-factor) to stronger forms, such as a combination of account and password in association with a token (3-factor). The strength of authentication is usually fixed, and additional possibilities for authentication (*e.g.* tokens and/or authentication using biometric factors) are limited, especially for public cloud services. Specific solutions are available (even in the form of cloud services!) that connect the internal authentication mechanism (usually MS Active Directory) to the provider's own authentication mechanism. This obviously requires additional investment and expenditure on controls. Besides that, authentication services over the internet is a niche market still in development, and its track record is limited.

Different authentication strengths, especially when authentication of the cloud service is weaker than the customer's requirements, can lead to weaknesses in the IT environment, with the result that the integrity and confidentiality of (financial) data is harmed.

When the required/desired form of authentication (*e.g.* a user account based on a specified convention, in conjunction with a password) is not applicable to cloud services, there is a high risk of incurring additional costs and management expenses. After all, two or more forms of authentication are being purchased and managed. Users should not be forgotten here. They have to log-on using extra and possibly other means of authentication in order to gain access to IT services. Multiple log-ons with multiple tokens and/or smart cards can be a very annoying experience, not to mention an additional management burden for the organization.

Single-Sign-On technology may in some cases be applied to establish a consistent form and strength of authentication, but it is generally difficult to implement, seldom fully applicable to all IT services, and often easy to circumvent insofar as cloud services are concerned, as many cloud services can be accessed directly from various access points on the internet.

In most large (more than 5,000 computer users) organizations, the processes for user management (creating, changing and disabling/deleting computer accounts) and authorization (who and/or which roles have which permissions for which data) of internal IT resources are complex and open to improvement. Frequently, this process has weaknesses such as obsolete but still active accounts, thus affecting security. Often authorizations for role/function changes within the organization include new permissions while the old permissions have not been removed, resulting in too many permissions and possibly infringing segregation of duties. This complexity is increased by cloud services that use different procedures and/or other technologies to facilitate these processes. Lack of integrated processes can result in further weak points, with negative consequences for the level of assurance.

Cloud services have their own access control and authorization processes that are, in principal, not directly compatible with the customer's requirements and wishes. Moreover, (open) standards for authorizations on computer systems are still in their development stages, while protocols such as SAML 2.0 provide sufficient latitude for a range of interpretations, thus hindering integration of different solutions.

Authorization mechanisms for more than 90 percent of purchasing organizations are based on the Security Groups and Group Policy Objects in Active Directory, which may or may not be supplemented by an RBAC tool. Both Active Directory and the RBAC tools are designed for an on-premise IT environment. Integration between different IT environments is therefore complex and still undergoing radical development. For example, Microsoft offers Active Directory Federation Services in order to integrate various Active Directories across multiple organizations. But this technology is also relatively new and not widely used on the market.

In practice, cloud-service authorization mechanisms tend to be independent of those of the internal IT environment. This situation therefore increases the risk of additional management costs, inconsistent processes and higher complexity. Integration with existing internal IT services and between different cloud-computing providers may entail significant integration problems and increase complexity.

This complexity also applies to other security mechanisms. Not only are there multiple solutions, the chain of which is only as strong as its weakest link, but the integration of security often results in compatibility issues and unclear responsibilities.

Given the technology currently in development, mitigating the indicated risks will mainly involve the area of process integration. An effort is also being made to harmonize provider and customer processes regarding access control and authorizations. Similar harmonization may also be a solution for private cloud services. In the case of public cloud services, the cus-

On-premise IT	Cloud computing	Cloud computing risks
Harmonized degree(s) and form(s) of authentication	Divergent degrees and forms of authentication between the customer organization and the provider	• Weaker authentication, leading to undesired concession in security • Bypassing of authentication mechanism, leading to security vulnerabilities
Harmonized control processes	Complexity of integrating control processes	• Too many permissions, leading to breach of segregation of duties • Uncontrolled growth of obsolete user accounts and permissions, leading to deficiencies
Harmonized authorization	Technical complexity of integrating authorization mechanisms	• Multiple instances to control authorizations, leading to additional costs and management burden • Integration based on immature technology, leading to unstable environment susceptible to errors

Table 2: **Cloud computing risks to access control & authorization**

tomer will have to submit to the provider's processes. In any case, this factor must be included in the business case.

It is therefore recommended that the following steps be taken before moving to the cloud:

- Identify current processes for user management, authentication and authorization.
- Define clear requirements regarding management processes, especially concerning authorization management.
- Define clear technical requirements, especially in terms of (open) standards.
- Define the future integration of technical architecture before making a choice.
- Perform technical pilot studies prior to selection.
- Define exit/migration strategy.

Change management

Concerning change management, two characteristics related to the risk profile of cloud computing apply. IT resources on the provider's premise means, in the first place, that changes on the IT environment with potential impact on the data are no longer controlled by the customer but by the cloud service provider. Unlike on-premise IT, change management in the cloud is primarily not the customer's responsibility but that of the cloud service provider.

Secondly, this also means that the customer only has limited influence on the changes in the cloud services that it purchases. In principle, the provider supplies all patches, new versions, and keeps the IT environment available. Multi-tenancy implies that each change has impact on multiple customers, thus limiting the degree of customization and desired time frame of changes.

The principle of multi-tenancy has the advantage of outsourcing complex change management to a specialist as well as more efficient way of implementing changes (one change which applies for multiple customers). The disadvantage is that the customer depends entirely on the provider's willingness and capacity to perform the required/desired changes. Moreover, undesirable changes cannot, in general, be undone for a single customer, especially when the service has a high degree of multi-tenancy. Although this especially applies to public cloud services, most private clouds are also highly standardized compared to on-premise environments.

In practice, it turns out that the limited control over and grip on changes does not impact the degree of assurance as much as the extent to which the provider grants access to its change management processes, that is: offering transparency. Few providers are openly transparent about the ways in which they manage changes on their systems and only provide useful information about future releases on their cloud services. Generally, there is a persistent lack of clarity regarding how and on what grounds changes are initiated, how the impact analysis is conducted, how a change is tested and how it is approved.

Good SAS70 – after mid 2011 SAS70 standard will be replaced by ISAE 3402 standard – reports seem to offer a solution to this issue, but only a minority of providers engage independent parties to regularly perform external audits. Moreover, the selected IT controls are often based on single-tenant structure and not the multi-tenancy characteristic of cloud services. Many of the controls necessary to ensure segregation of the data and resource utilization of various customers are not selected and therefore rarely audited. Furthermore, the auditor is faced with the problem that current frameworks, such as ISO27001/2, are hardly suitable for multi-tenant environments. New frameworks with new IT controls are currently being formulated, but the number of initiatives remains large without any of the frameworks being widely accepted on the market.

A right-to-audit is recommended in these cases, but its exercise is reserved for the most wealthy and/or influential customers. Few requests for audits are honored and many auditors lack the technical knowledge and experience with the architecture to evaluate cloud services on their proper merits.

Insufficient assurance from the provider can therefore constitute a reason to (temporarily) refrain from using cloud services.

On-premise IT	Cloud computing	Cloud computing risks
Changes initiated, authorized and generally implemented by the customer	Changes initiated, authorized and generally implemented by the provider	• Undesired changes • Unannounced changes
Change management controls aligned with relevant standards and regulations	Change management controls as defined by the provider	• Insuffficient assurance on adequate change management controls • Irrelevant standards as starting points for audits

Table 3: **Cloud computing risks to change management**

It is therefore recommended that the following steps be taken before deciding to move to the cloud:

- Identify change management controls with regards to applicable rules and regulations.
- Define clear requirements regarding the change management process.
- Demand right-to-audit where possible.
  - Use additional controls which apply for multi-tenant environments.
  - Make sure audits are performed by experienced auditors understanding cloud services.

Backup & recovery

Backup and recovery in the cloud also depend on measures taken by the provider. Apart from – often standardized – reports on backed up data, customers have to trust that the providers actually back up their data and store it in a safe place under proper storage conditions. In addition, customers have to assume that, in case of emergency, the backed up data can be instantly recovered and its availability quickly restored.

Several major incidents have demonstrated that not all data in the cloud is backed up adequately. Thousands of customers lost their data in the cloud due to the infamous "Sidekick Disaster" at Microsoft and T-Mobile in 2009. In violation of agreements, it turned out that Microsoft and T-Mobile did not fully back up the data of their customers. Furthermore, the part that had been secured only became available after several days.

Besides the issue of failing or missing backups, the use of subcontractors has also become a problem plaguing the cloud. Often, a portion of the cloud services is subsequently outsourced by the provider to other cloud computing providers. It is not uncommon for backups and archiving to be performed by other (specialist) providers in different geographical locations with different regulations concerning data storage, data protection and privacy.

For instance, an important part of the data from a US hospital using a cloud service offered by a US provider turned out to be archived in India. This was a violation of US legislation as it is prohibited to store medical records with personal data outside the US. The US provider had in fact outsourced its archiving activities to an Indian company without informing its customer.

The issue becomes critical when the cloud computing provider is no longer able or no longer willing to make the customer's data available to the customer. Possibilities for escrow exist, but besides the technical implications concerning recovery of data in the proper format and media, the market has yet to elaborate on legal and technical implications. For example, open data formats which can be interchanged (theoretically) between different technical solutions are seldom enforced and as of 2011, many data in the cloud is in proprietary formats of the provider in question.

A right-to-audit with regard to backup and recovery is recommended, but in practice, only a few requests for audits will be honored. Firstly, it is practically impossible for large providers to have their IT environment constantly audited by thousands of different requests. Secondly, auditing a multi-tenant environment requires specific expertise by auditors regarding architecture and technology which is sparsely available. Therefore, it is better to require transparency from the provider prior to making the purchase.

On-premise IT	Cloud computing	Cloud computing risks
Backup within controlled, internal perimeters	Backup outside customer's perimeters	• Conflicting legislations • Incompliance due to lack of transparency
Customized settings regarding backup & recovery meeting user requirements	Standardized measures of the provider	• Insuffficient service guarantees such as backup media and recovery time • Excessive backup data such as privacy-related data

Table 4: **Cloud computing risks to backup & recovery**

The following steps must therefore be taken before deciding to move to the cloud:

- Require proper agreements and SLAs with clear thresholds such as recovery times.
- Obtain a full list of all the parties in the ecosystem of the cloud (which parties are involved?).
- Identify applicable regulations on data, data protection and privacy on all physical locations of your data in the cloud. Take adequate legal measures.
- Arrange for escrow.
- Require open data formats and open standards where possible.
- Demand right-to-audit where possible.
- Define exit/migration strategy.
- Make sure that a risk analysis is performed in advance.

Conclusion

The share of IT expenditures allocated to cloud computing – notwithstanding the hype – is still marginal in terms of total spending on automation, and traditional, on-premise IT will be the dominant factor for the time being. Yet the emergence of cloud computing cannot be ignored: its growth is impressive and the model itself can be seen as the next phase in the process of centralization and consolidation of IT that began during the last decade. CRM, e-mail and storage from the cloud are already becoming de facto standards in automation, and more services will follow.

The impact of cloud computing on the degree of financial assurance should be put into perspective. On the one hand, cloud computing is mainly based on technologies that already exist, such as virtualization and web services, so existing IT risks apply. On the other hand, cloud computing has characteristics that considerably affect the risk profile, compared to the traditional, on-premise IT. These characteristics are:

- external data storage and processing;
- sharing of IT resources with other customers (multi-tenancy); and
- dependency on the public internet.

When we look at the main factors related to assurance in financial statements, namely access control and authorization, change management, and backup and recovery, we can determine that cloud computing harbors risks for the customer and challenges for the auditor.

Discrepancies between access control and authorization requirements of the customer and of the cloud computing service provider in technical and process-related fields can strongly influence the degree of assurance. Methods to integrate different directories are in their early stages of development while standards to align multiple cloud solutions are yet to be determined. In terms of process, the same applies to change management, which occurs virtually out of the customer's sight and control. With regard to backup and recovery, the customer must be aware that data is not necessarily stored just on the premises of the primary provider and that data recovery may be subject to significant technical and legal complications.

Although measures can be taken to mitigate the risks of cloud computing, on occasion it will be exceptionally difficult or even impossible to implement these mitigations, as a right-to-audit is rarely granted by big providers and current audit standards lack specific controls related to cloud services. In any case, the customer must have an exit/migration strategy ready at all times, enabling it to switch to alternatives at any moment. A thorough risk analysis in association with the development of a business case prior to the adoption of cloud computing is a matter of course.

The rise of cloud computing is seemingly unstoppable, even in the domain of financial business processes. As we speak, organizations are already moving their applications from their traditional, on-premise environments to the cloud. Awareness of this paradigm shift followed by adequate risk management will be a critical success factor.

References

[Chun09] Mike Chung, *Cloud computing als panacee*, KPMG, 2009.

[Chun10] Mike Chung, *Audit in the Cloud*, KPMG, 2010.

[Isac09] ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, ISACA Emerging Technology White Paper, 2009.

[KPMG10] KPMG Advisory, *From Hype to Future: KPMG's 2010 Cloud Computing Survey*, KPMG, 2010.

[OECD10] OECD Information Technology Outlook 2010, OECD, 2010.

[Schn09] Bruce Schneier, *Schneier on Security*, 2008.

[Shaz10] Shay Uzery and Joep Ruiter, *Privacywetgeving belemmert cloud computing*, Automatisering Gids, March 2010.