What is cloud computing?

The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This definition of cloud services can be divided into four parts:

- Service provision model
- Service access
- Service resources
- Service characteristics

Service provision models

Over the years we've seen that companies want to consume more and more things as a service. What is consumed as a service can either be very technical, such as IT infrastructure, but can also be very functional, like a Business Process. Typically, there are two drivers behind this need for a service consumption - the centralization/decentralization pendulum and the level of abstraction cloud services provide. The common denominator between these drivers is the cost and efficiency optimization of these cloud services. This also debunks the myth that cloud computing is only about technical aspects of enterprise architecture.

These drivers can be translated into cloud computing models grouped in two generations.

1st generation:

Focus is technical and linked with technology and application layers of enterprise architecture:

- Technology architecture -> IaaS (Infrastructure as a Service) and PaaS (Platform as a Service): focus on hardware, software and middleware.
- Application architecture -> SaaS (Software as a Service): focus on the use and customization of software, whereas the technical aspects are considered a 'black-box'.

2nd generation:

Linked with the information and business architecture levels of the enterprise architecture:

- Information architecture -> INaaS (Information as a Service) is all about managing data: creating, exchanging and extracting meaningful information.
- Business architecture -> BPaaS (Business Process as a Service) where the service entails wrapping a business process from beginning to end.

Service access

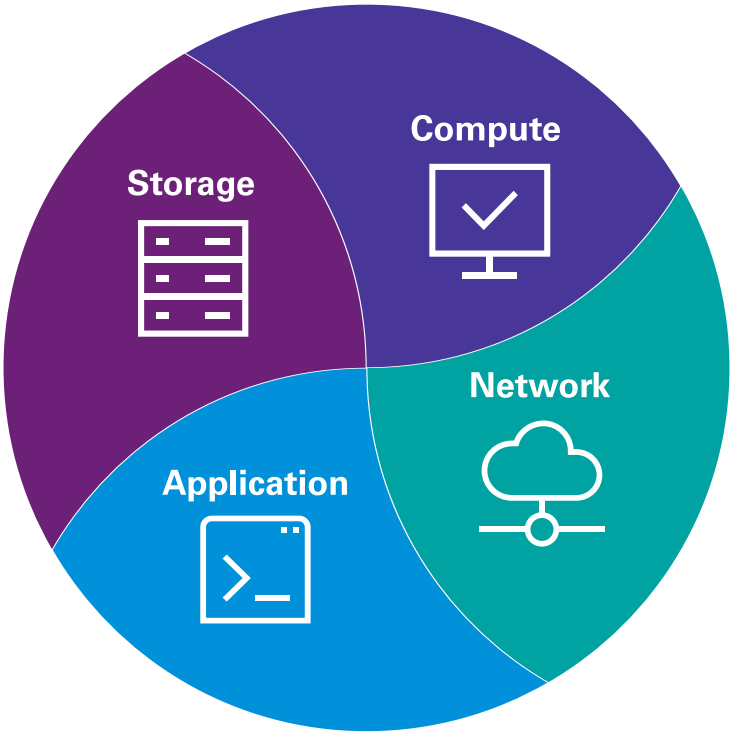
Another myth to debunk is that ‘network accessible’ means ‘internet accessible’. Although most of the cloud services are organized outside the organization and accessed over the internet, it is not a necessary condition. Cloud computing can be organized on the premises as well.

Deployment models are the different ways cloud services can be accessed. Typically, five models can be identified. There are (1) the private clouds which give access to a single entity and (2) the public clouds which provide access to anyone with internet access. In addition, there are (3) community clouds which provide the middle ground between a private and public cloud, (4) hybrid clouds which is a mix of previous models and (5) multi-clouds which is a consuming cloud for multiple providers.

Furthermore, in cloud computing there are four parties involved: the service provider, service creator, service consumer and service broker.

Service resources

- Compute: processing power or how many central processing units (CPU) can be provided to solve the problem.
- Storage: storing data but also the search to locate data in vast amounts of available data - includes structured (tables and databases) as well as unstructured data (images and documents).
- Network: to get data in and out of the cloud we need to connect to networks. Managing these connections is what the network resources do. There is another related cloud myth: cloud will still require some local-IT resources - at least a bare minimum - to organize the interconnection between on-premises and the cloud.
- Applications: a bunch of services needed to run the application in the cloud, for example, role-based security, access management, audit trails and logging.



Service characteristics

- Where: clouds can be accessed anywhere.
- When: available on-demand, so you can consume whenever you want.
- What: the pooling of resources for optimal usage; thus allowing cloud services to be efficient.
- How: horizontal and vertical scaling. Horizontal scaling means adding a greater number of the same resource. Vertical scaling means adding more performance to the same resource creating bigger resources; thus allowing the cloud to be effective.
- How much: how much you use is directly translated into how much you pay, so you pay for used capacity and not for provided capacity.

A myth linked to the service characteristics: since a cloud provider describes what services are available but does not prescribe how to use it, cloud will still require business-Information and communications technology (ICT) alignment.

Why cloud computing?

The reasons for cloud computing can be explained by four key ICT drivers:

Need for more ICT flexibility

- Staff can access resources from anywhere; for instance, allowing the possibility to work from home.
- Increasing and reducing resources without having to plan upfront; avoiding ICT investments that could otherwise require substantial financial resources.

Need to increase ICT speed

- The speed at which ICT can turn around its own processes and how it deals with frequent requirements changes.
- With cloud computing, change is not exceptional but rather business as usual; ad-hoc infrastructures become possible without a heavy overhead.

Increased flexibility and speed allow ICT departments to meet targets and support innovation and modern software development methodologies.

Need to reduce ICT costs

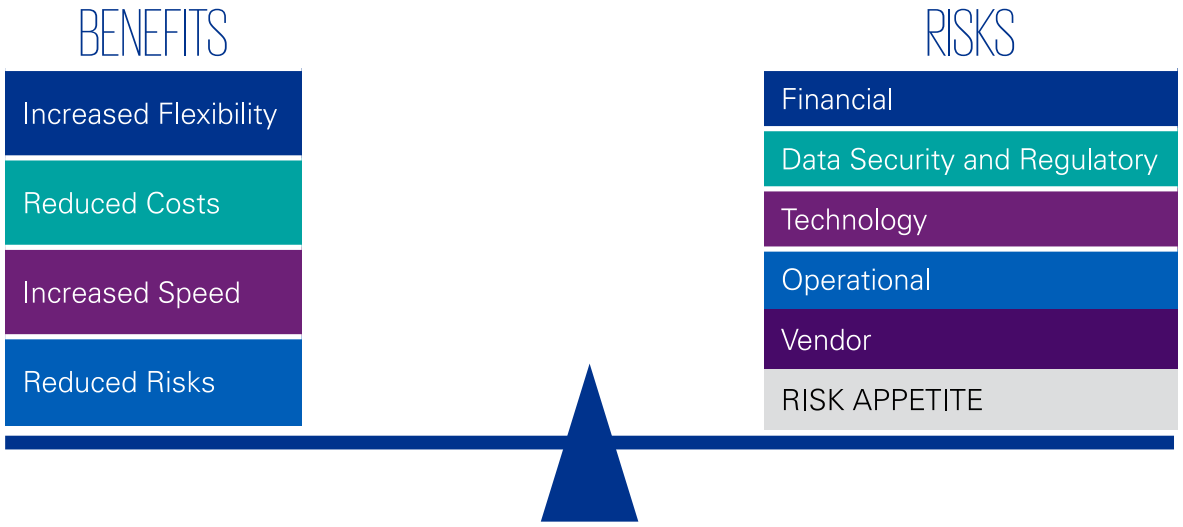
- Lower infrastructure costs:
    - Cloud allows for new IT infrastructure price and cost models that lead to a CAPEX to OPEX paradigm switch, reducing capital needs for IT.
    - Scaling allows for capacity and performance on demand, balancing the sunk-costs of idle capacity and the opportunity cost of missing capacity.
    - Economies of scale for cloud resources at the level of the cloud service provider reduces the costs for individual service consumers.
- Lower operational costs:
    - Costs of redundant equipment to guarantee availability, failover and business continuity is spread across all cloud service consumers of a cloud service provider, and not borne by a sole customer.
    - Part of the operations and management of infrastructure is taken over by the cloud provider, reducing the need to rely on in-house resources and knowledge.

Need to reduce ICT risks

- Reduced security risks:
    - Part of the responsibility and controls are moved to the cloud service provider.
    - Cloud services are compliant with industry accepted standards, including security risks and controls.

- Specific and specialized infrastructure related competencies are provided by the cloud service provider and do not have to be developed by the cloud service consumer.
- Reduced operational risks as a result of an extra set of eyes monitoring the platform.

Reduced risks and costs allow ICT departments to meet their targets which comprise a budget responsibility and a security and vulnerability responsibility.



Cloud key risks & considerations

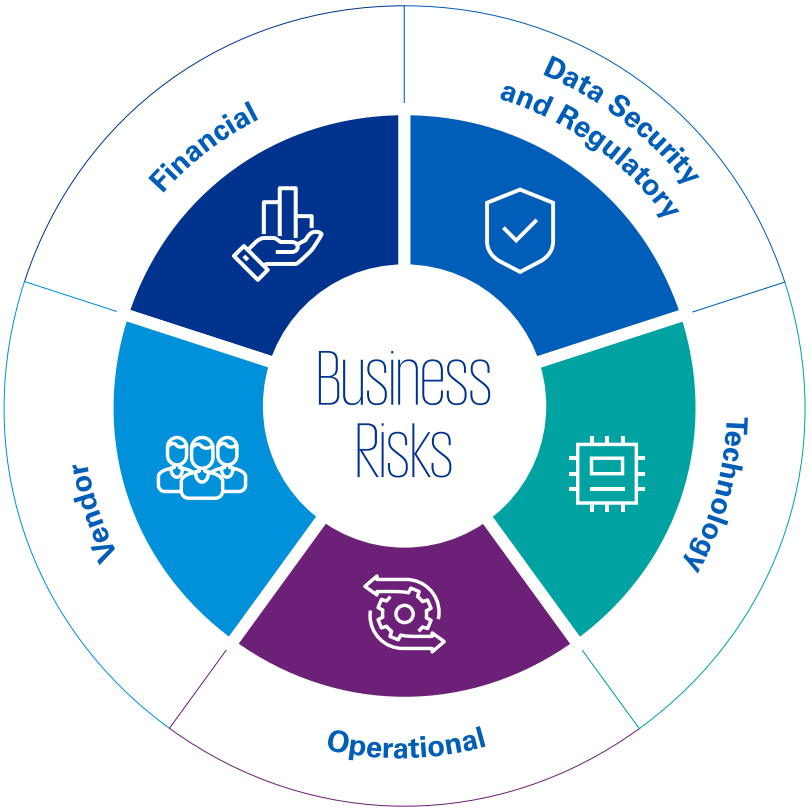
Despite its benefits including the reduction of risks due to the use of out-of-the-box solutions and involving trusted providers, it should however be clear that cloud computing may also introduce additional risks. The main reason for that is the fact that the company gives up control over its data and IT environment - at least to some extent, depending on, amongst others, the applicable service model.

The risks cloud computing introduces should be approached holistically across people, processes and technology in order to better leverage the cloud computing initiatives.

The five major risks related to cloud computing are:

1. Data security and regulatory: failure to meet regulatory compliance requirements (including across multiple geographies);
2. Technology: failure to identify vulnerabilities to security threats leading to loss, leakage and the unavailability of services;
3. Operational: failure to implement new cloud controls which are fundamentally different from earlier implemented controls;
4. Vendor: dependency on third party vendors and, for example, the applicable service model;

5. Financial: failure to perform proper cloud spend management around unplanned spikes in transaction volume and traffic.



As managing the risks of cloud becomes an increasing priority for organizations, the following areas also need particular attention:

The internal audit role in cloud computing

Through its key role as assurance provider, internal audit (IA) is well positioned to help management as well as the Board identify key risks related to cloud. IA can assist the business in determining whether those risks are being appropriately mitigated.

Internal audit should embrace the “trusted advisor” role as the organization takes on new risks and:

- proactively offer a balance of consultative and assurance services;
- educate and engage with the Board/Audit Committee; and

- have a forward-looking mindset to remain compliant with all relevant regulations.

Challenges in auditing cloud computing

Cloud computing is a disruptive technology and impacts how an audit is performed. Cloud audit challenges include:

Definition of scope

Understanding the scope of the cloud computing environment:

- which service and deployment model is utilized? Is the cloud service limited to infrastructure only or does the service also include databases and applications?
- where does the ‘cloud’ start and stop? Are processes fully supported by the cloud or is there a mix of cloud and internally hosted systems?

Dependence on third parties

- As cloud services are provided by third party vendors, there can be challenges in auditing areas that are under the control of third parties.
- Particularly for large cloud providers, such as Microsoft and Amazon, who have more commercial power than most of their clients, internal audit may need to gain assurance from other sources such as external certifications; it may not always be possible to include or exercise ‘right to audit’ clauses.

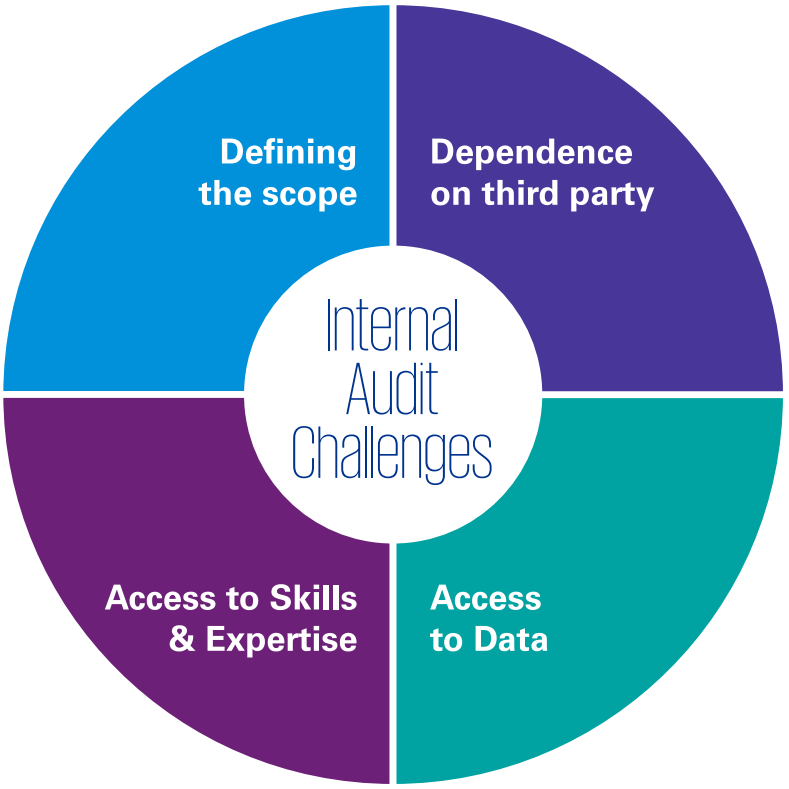
Skills & Expertise

Cloud computing audit specialists, on top of standard audit skills, should possess the following skills:

- knowledge of cloud service and deployment models;
- knowledge of organizational relationships;
- sufficient functional and business knowledge to assess alignment with the business state;
- knowledge of system architecture; and
- security knowledge.

Access to data

Testing the effectiveness of controls in through use of audit logging and audit trail may not be so evident in a Cloud environment compared to the traditional IT as this data may not be accessible to the organization. Access to it may require special agreements with the Cloud provider.



Key take-aways

- Cloud computing provides a lot of benefits and risks;
- While some risks can be reduced, other (specific) risks can emerge;
- These risks are more than an IT problem and can pose a threat to the business;
- Internal audit may play an important role in providing assurance, educating senior management and ensuring regulatory compliance;
- While the vendor's assurance reports can be used, internal audit should ensure all risks are covered by the report.

Dirk Vanderbist **Senior Manager** Digital Enablement - Cloud & Architecture **T:** +32 (0)27083967 **E:** dvanderbist@kpmg.com	**Thomas Vormezeele** **Senior Manager** Digital Risk Management & Assurance **T:** +32 (0)27084853 **E:** tvormezeele@kpmg.com

For more detail about the structure of the KPMG global organization please visit https://home.kpmg/governance.