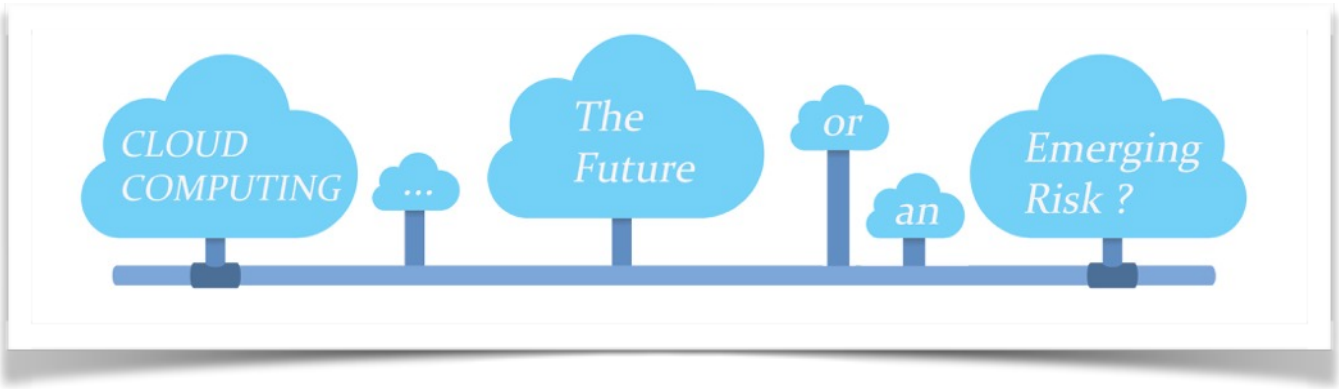

This article aims to provide an introduction to the concept of cloud computing, its associated benefits and risks as well as internal audit's role in the review of some of the key risks.

Cloud computing has been the buzzword, particularly in recent years. A 2018 cloud computing study[1] by IDG Communications has found that 73 percent of the 550 surveyed organisations have at least one application or a portion of their computing infrastructure already in the cloud. Locally, even the Singapore government has announced that they are expecting to move some of its IT systems to commercial cloud services over the next five years in ongoing efforts to deliver citizen services in a faster and cheaper way. Forrester Research estimated the global market size for cloud computing to be US$241 billion by 2020. Public cloud will constitute two-thirds of that market size, or US$159.3 billion.[2]

Yet, interestingly enough, cloud computing is essentially not a new concept, but rather one that has evolved into the more mature cloud industry today. Most of us use cloud computing without realising it when we access web-based applications like Facebook, Hotmail or Google Docs. The key difference today is the greater adoption in cloud services and its broader variety of usage due to better understanding of the model and increased consumer confidence with the security of cloud service providers.

What is Cloud Computing?

The National Institute of Standards and Technology (NIST), which is a non-regulatory agency of the United States, defines Cloud Computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [3]

---

[1] IDG 2018 Cloud Computing Survey https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/

[2] Infocomm Media Development Authority Cloud Computing - IMDA

[3] The NIST Definition of Cloud Computing - Special Publication 800-145 https://csrc.nist.gov/publications/detail/sp/800-145/final

Broadly, there are three main service models:

* **Software as a Service (SaaS)** – Consumers are given access to the service provider's applications that run on a cloud infrastructure and the management of infrastructure, operating environment, platform services and application configuration is left to the cloud provider. These may include email, Microsoft 365 and Customer Relationship Management software like Salesforce.

* **Platform as a Service (PaaS)** – Consumers are given access to develop and deploy their own applications in the environment that operates in the service provider's hosted infrastructure. The PaaS provider takes care of delivering the programming platform and all underlying software and hardware infrastructure. Google AppEngine and Microsoft Azure are examples of PaaS.

* **Infrastructure as a Service (IaaS)** – Consumers are provided a virtual data centre of resources that allows them to install software and set up applications. The IaaS provider takes care of the server hardware and network. Responsibility of maintaining the operating system usually falls on the consumer.

In addition, there are four types of cloud infrastructure models :

This is operated solely for a single organisation. It can be managed by the organisation or a third party and can be hosted within or outside the organisation's premises.

This is operated by a cloud provider and is available for public consumption. These are multi-tenant clouds serving a variety of customers that usually enjoys the largest scale and utilisation efficiency.

This serves a specific industry or community that shares a common trait or set of concerns (e.g. security and compliance requirements, or a certain common application). It can be managed by the organisation or a third party and can be hosted onsite or offsite.

The cloud infrastructure is a composition of two or more cloud deployment models that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability.

Benefits of Cloud Computing

The key benefits are the quicker deployment of solutions that reduces the time to market which helps the organisation to achieve their objectives, greater scalability, enhanced resilience, efficiency and cost savings.

The traditional approach for in-housed technology was such that organisations would run all applications on own servers hosted in data centres within their premises. This naturally involved significant investment for new applications, ongoing maintenance and upgrades to ensure that the data was securely held. With cloud computing, solutions can be readily available as the vendor is equipped with the expertise and tools to support the organisation. A cloud set-up also takes advantage of the economies of scale with a reduction in costs per server and distribution of application management costs between tenants in the cloud for multi-tenancy arrangements.

Cloud computing also tackles the scalability issue upon demand. Some businesses are more suitable for cloud such as online retailers when demand peaks during sales. The business would require sufficient technology infrastructure capacity to withstand the demands for such peaks, but it does not make economic sense to maintain servers with huge capacity just to fulfil the demand a few times a year. Cloud computing thus has a unique advantage as it can expand based on dynamic needs and shrink when not required so the consumer only pays for what is used.

Furthermore, the majority of the technology infrastructure costs are classified as capital expenditure with yearly depreciation and often the organisation does not fully utilise the resource capacity. Whereas, with cloud computing, the business is paying for what it's using which is accounted for as operating expenses without a depreciation cost.

Associated Costs and Risks with Cloud Usage

Security, data protection and outsourcing risks are some of the key risks associated with cloud usage and continue to be the main challenges when implementing a cloud computing strategy. The organisations together with the service providers are still expected to meet the regulatory and compliance requirements when adopting cloud services.

Data manipulation, loss or theft has often been a top security concern when considering adoption of cloud computing. While these risks exist for the traditional approach, there is heightened sense of concern driven by i) the fact that cloud services are provided by vendors and there is often no right of audit and reliance has to be placed on the vendor's independent review reports, ii) the inherent risk of multi-tenant environments where there are concerns over service providers' ability to segregate client data effectively and iii) evolving regulatory landscape for data protection rules, including cross border data transfer restrictions. The organisation would suffer considerable reputational damage and potential regulatory fines and implications should there be such data leakage or manipulation incidents. Some high-profile incidents associated with the security configuration of cloud include those relating to Apple[4] and Amazon Simple Storage Services (S3)[5] that supports a number of organisations and holds sensitive information. These incidents resulted in exposure of confidential data of millions of individuals and in some instances sensitive corporate information, highlighting the risks associated with cloud data storage and the need for strengthened security controls.

---

[4] Apple iCloud Incident https://www.esecurityplanet.com/network-security/apple-admits-celebrity-accounts-were-hacked-but-denies-icloud-breach.html

[5] Amazon S3 Incidents https://businessinsights.bitdefender.com/worst-amazon-breaches

While there may be cost savings from the technology perspective, there is a potential increase in costs and risks from the establishment and management of vendor outsourcing as well as the migration to new processes. New contracts together with service level agreements have to be established which state clearly the roles and responsibilities of the vendor and the organisation, penalties, fees, key performance indicators, governance model for the outsourcing arrangement and business continuity measures. These would need to be monitored by the organisation and issues escalated to senior management when necessary. A change to cloud computing may also require refinement in internal processes within the organisation to allow for seamless integration and in some cases the migration of legacy applications can be complex. There is a risk of vendor lock-in which makes the consumer dependent on the vendor for the cloud service and once the service is outsourced, there can be a lack of transparency in how it is managed, the employees engaged to manage the data or if the cloud provider subcontracts processing of such data. There is also a need for continuous access to internet to support the use of cloud applications. Organisations should also be cognisant that the SaaS model may not support customisation of the applications if required, compared to the traditional approach where the in-house IT could customise the application based on internal needs.

With the risks in mind, it is therefore important for organisations to assess what should be stored in cloud, in which country the data will be stored, how the data will be accessed and managed together with the security controls in place. It is also vital to assess if the approach fits in with the overall strategic objectives of the organisation and whether the vendor is deemed to be reliable after due diligence reviews. Ultimately, the responsibility to ensure that the above risks are addressed still lies with the organisation and does not get transferred to the vendor.

The role of Internal Audit

It is important to note that cloud computing risks are not limited to technology. Besides the greater dependency on third parties which requires organisations to establish a robust governance framework for the outsourcing arrangement, the greater magnitude of privacy risks and increased complexity of compliance with laws and regulations also require organisations to carefully consider the additional challenges from commingled data, cloud data ownership, and cross-border flow of personally identifiable information.

Auditors need to have a holistic view of the associated risks in order to effectively evaluate the basis for decisions and assessments made by the organisation on cloud computing implementation. The cloud exit strategy should also be carefully assessed as it is important for organisations to formulate plans to enable them to retrieve, restore and remove their data in a timely and orderly manner from their cloud providers when the needs arise.

Information Systems Audit & Control Association (ISACA) has also published a guidance titled “IT Control Objectives for Cloud Computing” that outlines the cloud computing fundamentals and an assurance programme.

Locally, the IT Standards Committee has published TR30: Technical Reference for Virtualisation Security for Servers, and TR31: Security and Service Level Guidelines for the Usage of Public Cloud Computing Services. TR30 arms enterprise infocomm personnel, cloud service providers, cloud users and buyers with a set of guidelines and best practices to address security risks posed by virtualisation based on compute hypervisors. TR31 provides security and service level guidelines to be considered by users seeking public SaaS and IaaS cloud services can use the standards as a starting point to evaluate the suitability of a particular cloud provider.

These are guidance that Internal Auditors can consider when reviewing the business case for cloud computing, vendor due diligence, if sound governance is in place with clear roles and responsibilities, documented policies and procedures and oversight controls. Internal audit's ability to provide independent assurance over these areas could help add value to the organisation and shape their strategy.

This article was contributed by the IIA Singapore Technical and Technology Committee comprising :

Nadiah Chang
Principal Audit Manager, Group Audit - Deutsche Bank

Henry Chan
Head, Internal Audit - NETS

Vincent Cheong
Executive Director, Group Audit - UOB Group

Sia Hwee Lay
Head, Business Audit - GIC