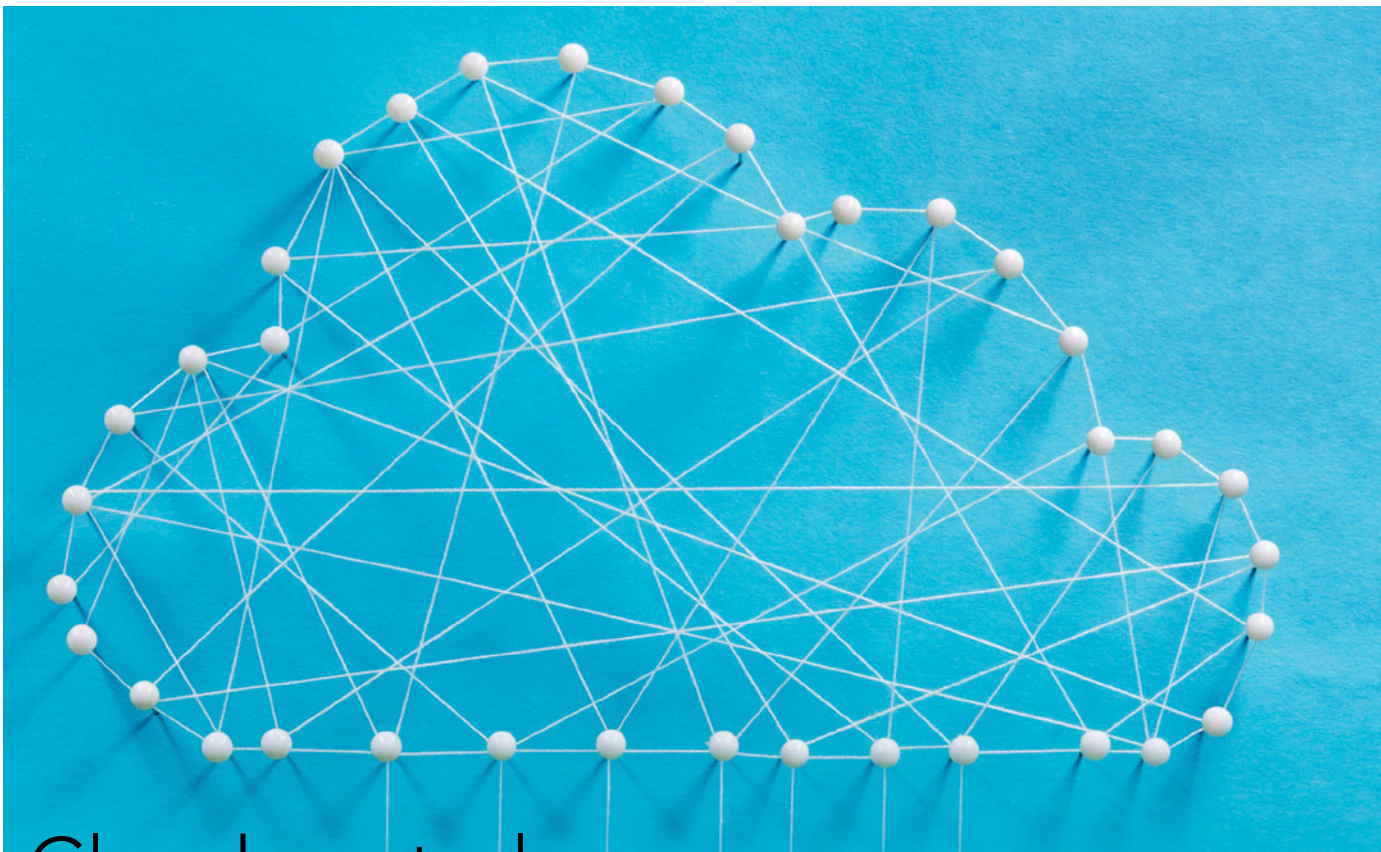


Cloud control

With cloud technology being increasingly viewed as the future for managing IT in the financial services industry, security concerns continue to loom large

For some years, cloud technology has been touted as the way forward for businesses to manage their information technology (IT) infrastructure. Underpinning the increasing popularity is the technology's ability to meet IT workloads and applications deployment without having to commit to the high cost of maintaining systems.

The benefits of the public cloud are clear for businesses. By having applications installed in data centres instead of being 'on premises', companies no longer have to individually install software locally on personal computers, laptops or tablets.

Data stored on central servers is more secure and is centralised for all to access. Organisations also do not need to worry about software upgrade cycles and users can access all their applications via the browser. Financially speaking, companies are able to move their IT spending from a capital to an operational expenditure model because they are consuming IT as a service and not buying hardware as assets. This means that IT budgets could become much more efficiently utilised.

But despite the obvious advantages, the financial services industry (FSI) is still struggling to come to terms with the concept, especially where it involves a third-party service providers' common data centre shared by many clients.

According to Teh Lip Guan, PwC Consulting Services executive director, security is still the main concern for public clouds and this is a major factor in causing banking regulators to be hesitant in pushing the approach in Malaysia.

'The central bank – in this case Bank Negara – is naturally more conservative and protective in its strategy and execution, as compared to those in Australia and European

countries, due to the economic and financial climate in the region,' he says, adding that with market economics and increased competition in the region, Bank Negara is being pushed to provide guidelines on the use of cloud computing. Elsewhere in the region, Teh notes that Singapore was the first regulator to issue guidelines on the use of cloud computing in South-East Asia, followed by the Philippines.

Quality and integrity

Steve Hodgkinson, research director for Ovum Asia Pacific, says that the main requirements for any public cloud service provider is that they must be able to assure the quality and integrity of their information system environment so that they will be able to meet regulatory requirements. It must be able to provide its services on a contractual basis, with service-level agreements (SLAs) clearly defined so that customers can have the confidence that operational requirements for availability, reliability and security can be safely met.

'These contracts must be able to be executed in the jurisdiction that the service provider is based in – that is to say, under local laws,' Hodgkinson says. 'This creates a strong preference for contracting with a locally based service provider and for keeping data in the country of its origin.'

Dan McConaghy, Asia Pacific president at FICO, an analytics software company, says that there is currently no one-size-fits-all set of central bank guidelines for public cloud computing services. 'The guidelines are as varied as the countries themselves, as many economies have banking systems that are still going through a period of automation and modernisation,' he says.

But what is clear, according to McConaghy, is that managing data privacy and sovereignty is a key imperative and focus for all the players – banks, regulators, technology solution and IT infrastructure providers – within the ecosystem.

'There are some very stringent regulations about the locality and ownership of data, including standards and best practices for the type of data moving through the cloud, how it's encrypted, how it's stored and transferred, and they are evolving and constantly improving,' says McConaghy.

While the FSI is at best cautiously optimistic about the potential of public cloud computing, some forward-looking banks in the region have begun to migrate parts of their IT workloads onto the public cloud. Examples include the Commonwealth Bank of Australia, National Australia Bank and Suncorp Group, all of which are using Amazon Web Services – one of the largest public cloud providers in the world.

> 'CONTRACTS MUST BE ABLE TO BE EXECUTED IN THE JURISDICTION THAT THE SERVICE PROVIDER IS BASED IN'

'Hybrid' adoption

PwC believes that while core and critical banking applications are unlikely to move toward public cloud deployment any time soon, there are 'hybrid' cloud adopters for selected services, namely the non-core and secondary banking activities such as human resources (HR) application, software development, procurement and customer relationship management.

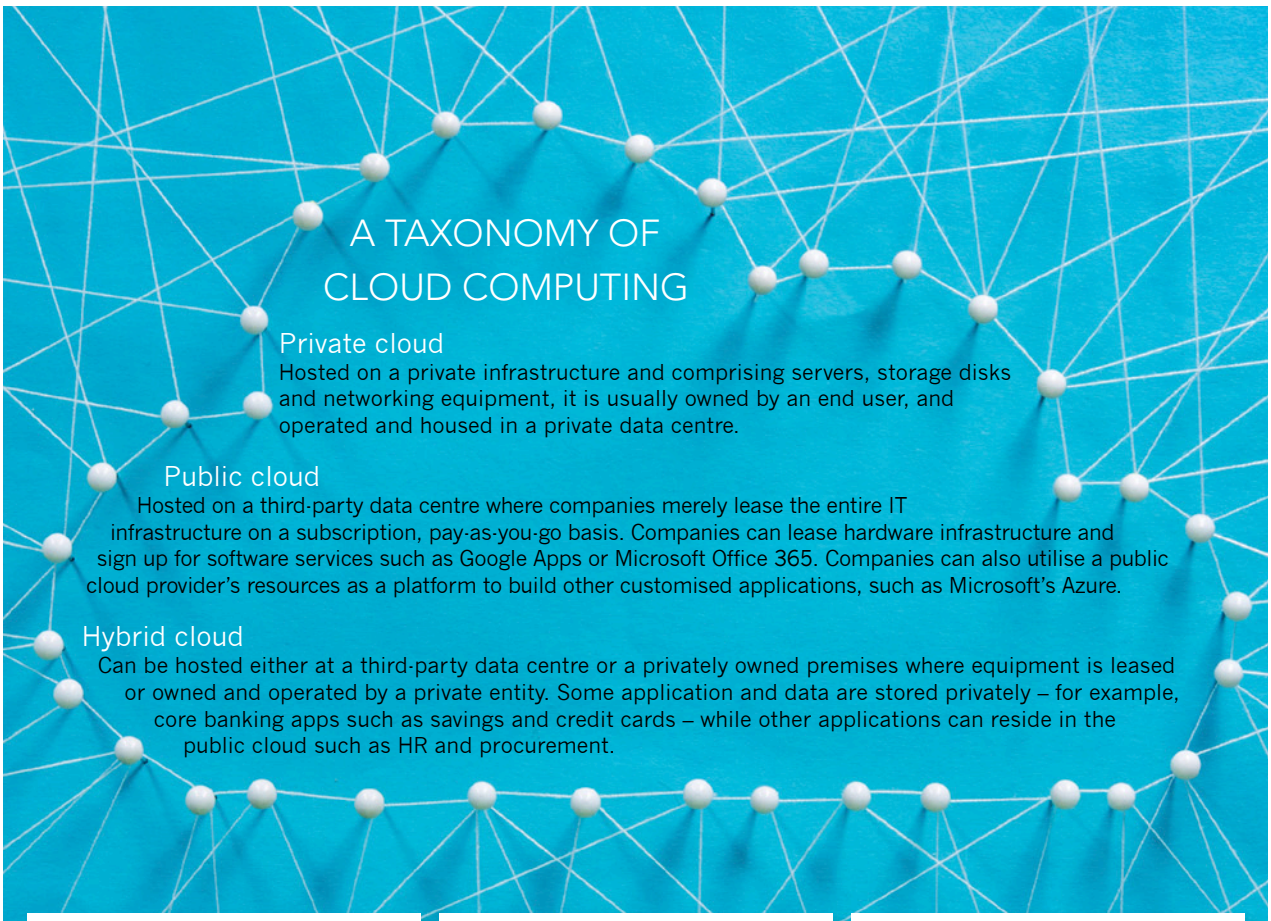
In Malaysia, one bank that has begun experimenting with public cloud services is Alliance Bank Malaysia. Since 2013, the bank has geared parts of its HR and internet protocol telephony applications onto the public cloud, explains Mary James, Alliance Bank Malaysia's group chief information officer.

Among the benefits of using a public provider are cost efficiency, value-added benefits without incurring additional costs, no upfront purchase of hardware, scalability of system, and lower carbon footprint through resource sharing, James says.

However, she points out, until the technology itself matures further and FSIs fully understand how service providers deliver their solutions, it's very unlikely that more banks and core applications will move to the public cloud.

FSIs can, however, choose to implement a partial move, as Alliance Bank has done with its HR and internet protocol telephony applications. 'There are many other solutions that banks can move to the public cloud without infringing on any guidelines, she says. 'Examples include recruitment, enterprise resources planning solutions and device management.'

James says that one of the main considerations for her bank was ensuring that the data being stored in the public cloud does not infringe on guidelines as provided by Bank Negara. 'We also needed to understand and learn about the service provider and the types of practices and processes being provided, as many service providers do not necessarily have the same types of strict guidelines and »



A TAXONOMY OF CLOUD COMPUTING

Private cloud

Hosted on a private infrastructure and comprising servers, storage disks and networking equipment, it is usually owned by an end user, and operated and housed in a private data centre.

Public cloud

Hosted on a third-party data centre where companies merely lease the entire IT infrastructure on a subscription, pay-as-you-go basis. Companies can lease hardware infrastructure and sign up for software services such as Google Apps or Microsoft Office 365. Companies can also utilise a public cloud provider's resources as a platform to build other customised applications, such as Microsoft's Azure.

Hybrid cloud

Can be hosted either at a third-party data centre or a privately owned premises where equipment is leased or owned and operated by a private entity. Some application and data are stored privately – for example, core banking apps such as savings and credit cards – while other applications can reside in the public cloud such as HR and procurement.

processes that the banks might employ,' she explains, adding that the bank will continue to explore further opportunities in this area.

According to Hodgkinson, there are no easy steps to follow to get on board with public cloud computing. Rather, it's a matter of gaining skills and experience progressively. Hodgkinson refers to the experience of Suncorp Group, which, while at the leading edge of cloud services today, had been testing its approach for several years using a range of private and public cloud arrangements.

'All about trust'

'It is all about trust, and trust is only gained with experience and skill,' he says. 'Think of it as like learning to drive a car. It is dangerous to drive while looking in the rear-view mirror; that's like living in the past. But it's also dangerous to drive too slowly because you fail to build the skills needed to drive in motorway traffic.

'The best approach is to develop defensive driving skills, which can only be done "hands-on". Banks need to try cloud services safely to build experience and skills in order to get hands-on with cloud services to learn the skills to be an intelligent customer,' he says. 'Regulators need to ensure that regulations are not unjustifiably conservative or parochial and are clearly communicated to banks.'

Teh recommends that banks begin identifying what needs to be protected before formulating security controls to protect the data from an end-to-end process workflow which includes the data creation process, transit, storage and usage.

'We recommend that banks develop a sound strategic framework prior to embarking on the cloud journey – one that spans strategy through execution and addresses the risks, security matters and compliance implications of the cloud,' he says.

Teh also believes that banking regulators must accelerate their efforts in guiding the FSI in adopting cloud computing.

'Any uncertain issues and doubts arising from the regulator must ideally be resolved,' he says. 'They must also be familiar with the strengths and limitations of various types of cloud computing, so that they are able to guide FSIs.' ■

Edwin Yapp, journalist