DISCUSSION PAPER

MOVING TO THE CLOUD FOR COLLABORATION

SEVEN KEY CONSIDERATIONS

The rapid evolution of public and private cloud computing has fundamentally changed the way Australian businesses design, procure and manage their IT and communications systems. Mature private cloud offerings simplify complex enterprise environments and public cloud services facilitate access to new applications and capabilities. Yet while cloud's potential benefits have never been greater, its risks need to be understood and managed if those benefits are to be realised.

Figures from Gartner confirm the market's strength: for 2013 it predicted Australian companies' spending on public cloud services would grow by 23 per cent, surging from US$3.2 billion to $US5.2 billion by 2016.[1]

That's a faster rate of growth than the 18.5 per cent annual global average[2] , confirming that cloud services in Australia are making their mark as providers and mitigating concerns about integration, security, migration and the robustness of cloud solutions.

A growing proportion of the cloud market relates to the provision of unified communications as a service (UCaaS), in which unified communications are delivered through a cloud model that reduces costs and simplifies management. Frost & Sullivan forecasts the unified communication services market in Australia will grow at 9.2 per cent per year through to 2020, by which time it will be worth over$800 million. [3]

Indeed, Gartner has also found that cloud is the number-one technology spending focus for Asia-Pacific and Japan organisations, with 31 per cent of regional CIOs investing significantly in cloud compared with 25 per cent globally. Cloud is strategically important, with Asia-Pacific and Japan organisations proving to be greater users of platform as a service (PaaS) and infrastructure as a service (IaaS) cloud services than the global average. [4]

"It's largely about business agility," says Brett Emmerton, Director, Cloud and Data Centre at Optus Business. "As the pace of business increases, the need for technology refreshes increases as well. That doesn't really align with three- to five-year on-premises procurement cycles, or five- to 10-year enterprise software license agreements. As business and markets ebb and flow, enterprises are finding they need infrastructure to be able to adapt much more quickly."

While customers are ready to buy cloud, most organisations are far less ready to implement it. IT Infrastructure Matters, a 2014 survey of 750 technology executives in 18 countries conducted by IBM, found that although 70 per cent of organisations recognise that IT infrastructure plays a significant role as a generator of competitive advantage or revenue, just 22 per cent of surveyed companies have a well-defined enterprise IT infrastructure strategy roadmap.[5]

The challenges are many, stemming from the need to navigate a complex, ever-changing mass of legislative, technological, political and executive requirements. IT and business leaders need to work together to build a cloud-enabled environment that not only keeps up with current requirements but underpins the company's entire future IT direction.

While each organisation's individual requirements will vary, their core goals will be remarkably similar. Each will go through a process of re-evaluation, planning, implementation and, with appropriate action, eventually success. As they move towards their goals, each needs to work through seven core considerations to make the cloud work for them.

1. NETWORK AND INFRASTRUCTURE READINESS

The potential cost savings of UCaaS and other cloud-hosted solutions are increasingly well known and accepted. Predictable IT costs, consistent quality of service, a high level of redundancy and scalable design all support the business case for cloud, says Armond Savazian, Practice Manager for Unified Communications with Optus.

"Businesses don't want to buy and own infrastructure that becomes end of life in a few years' time," he explains. "Cloud offers an opex rather than a capex model, which is more about predictability. It allows customers a high level of redundancy without the need to go build it themselves."

1. Gartner: Forecast Overview: Public Cloud Services, Worldwide, 2011–2016, 4Q12 Update, 2. Gartner: Forecast Overview: Public Cloud Services, Worldwide, 2011–2016, 4Q12 Update
3. Frost & Sullivan: Australian Unified Communications Market Report 2014, 4. Gartner: 2014 CIO Agenda: An Asia/Pacific and Japan Perspective, 5. IBM: IT Infrastructure Matters

However, deciding to commit to the cloud is only the beginning. A key consideration before any upgrade is to evaluate your existing infrastructure and assess what changes are necessary to ensure the migration can happen smoothly and seamlessly.

One significant consideration is the bandwidth of the wide area network (WAN) that will carry voice, data and video traffic to and from the data centre. Usage profiles must be established for each site in the organisation, with bandwidth overheads for anticipated growth.

If mobile access is planned, wireless LANs must also be evaluated to ensure adequate capacity for the service's demands. "If wireless has not been designed to support voice and real-time applications, that's got to impact the environment," Savazian says.

Such considerations are increasingly playing into organisational strategy, with infrastructure and data centre refreshes named as the second-highest area of concern for CIOs across the globe in Gartner's research.[6]

KEY QUESTIONS

- Which of your currently installed technologies will limit the performance or usability of cloud applications?
- How much bandwidth (fixed or mobile) is available to users at company locations or on the road?
- Can wireless and mobile services be effectively used to shift users' traffic away from fixed networks?

2. THE CHANGING ROLE OF IT

Implementing the organisational changes involved in adopting cloud can take months, but time isn't the only concern. In many cases, an even more significant change comes about as traditional roles are redefined or even completely eliminated.

IT leaders need to respond by embracing the cloud's business benefits – for example, its shifting of budget-heavy capex to budget-friendly opex.

Positioning cloud initiatives in the context of business savings will strengthen IT leaders' standing within the organisation and help them retain their relevance during the cloud transition.

"When we engage with customers, there's usually a healthy debate on where they are and where they want to be," says Howard Fyffe, Asia Pacific, Japan and Greater China director of sales and operations for cloud and data centre with Cisco Systems.

"One of the biggest challenges is to drive a consensus," Fyffe says. "You're pulling together people from the business as well as IT, security and compliance teams."

In one recent engagement, Fyffe says, "the IT group was just too IT-centric" but Cisco was able to map the business processes to a consumption-based IT model, set up a portal-based solution and introduce the right services.

Embracing and managing change has become essential for IT executives and managers. As well as 'keeping the lights on' – still a major part of their role – they also need to act as a cloud service broker, risk manager, security specialist, and identity manager. To complicate matters further, this multi-disciplinary role must be executed in a climate of shrinking capital budgets – which would typically be associated with shrinking influence in the organisation.

Resolving this conflict requires constant effort, but it's imperative that IT managers and teams adapt their roles and embrace – or better yet, lead – organisational change. To consolidate these skills, analysts talk about the increasing importance of new roles such as the chief digital officer (CDO), which is still a relative rarity in Asia-Pacific companies – only 11 per cent have appointed one, according to Gartner, though this is ahead of the global average of just 6 per cent. [7]

Over time, however, the CDO will grow in importance as a facilitator of the transition and the empowerment of business leadership in the world of cloud services. The most successful of today's IT leaders will be the ones that work within changing executive structures to help the organisation move forward as a cohesive whole.

KEY QUESTIONS

- How are your organisation's departments empowered to make decisions about IT strategy?
- Where are the roadblocks? Which business units or executives are proving to be averse to change?
- How can you position cloud investments in the context of the changing capex/opex balance, so that individual business units don't take advantage of their newfound flexibility to head off in their own directions?

3. SECURING COMMUNICATIONS IN THE CLOUD

A key concern for many organisations is the security profile of a hosted cloud solution.

"Security has come out as the number-one issue in a lot of our research," says Frost & Sullivan analyst Audrey William. "For many years, organisations have been so used to controlling information within their own premises, and having their IT departments managing it all in-house, that they find it confronting to consider the security of a cloud offering."

Indeed, research consistently shows that the majority of companies still don't know how to secure their businesses in the cloud. The PwC Global State of Information Security 2014 (GSIS) survey of senior business and security executives found that just 48.8 per cent of respondents across all regions had a cloud-computing security strategy in place. [8]

Overall, the cloud security picture remains challenging. With less than half of all companies reporting they have a good grip on cloud security, the risks of adopting the new technologies must be carefully managed. Certain forward-looking organisations recognise that cloud service providers like Optus have invested far more in data centre and application security than they could ever do on their own.

"At the end of the day, our cloud provider has much stronger security than I can afford," says Peter Smith, Chief Information Officer with Wolters Kluwer Global Shared Services, which recently began a major rollout that will see it relying on an external cloud provider to deliver its Software-as-a-Service (SaaS) accounting software to customers around the world.

"Customers want to know that we understand the privacy issues, understand that intrusion detection is in place, and that all the right ISO processes are in place," Smith says. "But doing those sorts of things in an internal, in-house environment just isn't viable anymore."

To provide this security, in modern cloud environments the customer's network is securely extended to the cloud service provider using encrypted virtual private networks (VPNs). Each customer gets its own secure virtual instance of the service being provided, which is logically separated from other instances and managed for security in its own right. This provides a logically secure infrastructure that can be extended across a large number of client environments.

KEY QUESTIONS

- How important to your organisation are issues of data sovereignty, and how can they be addressed?
- What kind of security protections have you put in place, and what are your vulnerabilities?
- How do you ensure that your partners and suppliers are secure, and aren't providing a back door into your network?

6. Gartner: 2014 CIO Agenda: An Asia/Pacific and Japan Perspective, 7. Gartner: 2014 CIO Agenda: An Asia/Pacific and Japan Perspective, 8. PwC: Global State of Information Security Survey 2014

4. REGULATORY ENVIRONMENT

Government agencies have long been sensitive to protecting the privacy of the citizens they serve, while private-sector operators in financial services, telecommunications, and other data-intensive industries may face similar requirements.

As a result, some organisations have held off on cloud because of concerns about the jurisdiction where cloud-hosted data is stored. In the process of ensuring compliance, organisations must carefully review the types of information they plan to store in the cloud service, the types of data that the service will generate, and those that the service requires to operate correctly.

For example, in many cases a UCaaS environment's data exposure is far less than may have been anticipated, according to Tony Hudson, NSW Government Manager with Optus.

"In a voice environment, it's a different and less risky form of data because it's really about call records, rather than a lot of stored personal data," Hudson explains.

It's also important to consider whether specific governance measures are legal requirements or best-effort guidelines. This can dramatically alter the way that data controls are implemented and managed.

For example, some cloud users may prefer to keep their data onshore in Australia even in circumstances where there are no legal controls requiring them to do so. This might be because onshore hosting gives peace of mind, facilitates access to data centres or ensures stronger support channels.

Cloud adopters must also consider the data-handling implications of ancillary processes such as technical support, which may require specific information be provided to offshore technical staff. In such cases, it's important to consider the regulatory controls that must be placed around such data.

"As clients become educated in the subtleties or demarcations in the data, they will understand that not all data is equal," Hudson says, noting that generic call records are different to personally identifiable information (PII) such as drivers' license numbers or birth dates.

"Most clients appreciate the only way service providers can deliver is by finding a lower cost base," he explains. "This is typically offshore for some portions of their service, and it comes down to demarcating the data: if it's not really critically sensitive, personal data, it may not matter to organisations as long as they are getting the benefits of the cloud service."

KEY QUESTIONS

- Have you done a full inventory of the data you hold, and determined which regulations apply to which data types?
- Do business processes such as offshoring involve transitions between regulatory jurisdictions – and if so, how does this affect your cloud strategy?
- What kind of controls can you apply to control the movement of data to and within the cloud?

5. INTEGRATION COMPLEXITY

One of the often underestimated challenges of the cloud transition is the integration of multiple services into a common operational platform. PwC GSIS respondents confirmed how difficult integration can be, with nearly 1 in 5 respondents naming poor integration or overly complex systems as a key strategic obstacle. [9]

"The reason people want to go to a cloud environment is because it offers lower operational costs and is potentially more reliable and flexible," Hudson says. "The reason it's so cost-effective is that you're sharing the infrastructure across multiple clients."

"Agencies at this point still want to see configurations specific to their needs, but over time – if they're really serious about driving efficiencies in all areas of their operations – they'll have to ask whether they really need a separate instance for each department."

The issue has been compounded by the requirement to service multiple channels – mobile, Web, phone and others – with a consistent user experience. This is where the cloud environment offers considerable improvements over legacy approaches: by building on consistent and repeatable platforms, a cloud-hosted solution can help organisations reduce the complexity of a hosted environment while tapping into cloud's economies of scale and ability to span multiple environments with a single upgrade path.

Careful planning is required. Kevin Bloch, Chief Technology Officer at Cisco Australia, has seen underestimation of the integration burden create unexpected problems for all manner of organisations. Similar roadblocks abound during the cloud migration, which is why it's important to take a holistic look at existing and planned services to ensure there is a clear migration and integration path.

"Many organisations underestimate the transformation that IT-as-a-Service requires internally," Bloch explains. "First, there's the impact of the migration from on-premises IT and then there are the changes to business processes."

"Businesses need to look at how cloud or hosted services affect the supply chain from the customer through the organisation. This often cuts across business functions, and this means big changes to processes and to how people work."

KEY QUESTIONS

- How broad and complex is your current environment?
- How could universal access to unified communications facilitate technical or functional links between disparate parts of the business or infrastructure?
- At what point would integration become so complex that starting afresh, with modern and capable cloud alternative, would be the best option?

6. MIGRATION AND TRANSITION

The decision to migrate an entire infrastructure to the cloud is not one to be taken lightly and once it's made, migration often proves a significant challenge – both for technical reasons and employee resistance to change.

For example, the new environment may be no less complex than the old. Indeed, as it's likely to be a hybrid of cloud and conventional solutions, it may even be more complex.

"Adopting multiple cloud services for different applications or business functions can actually result in a more complex environment," Emmerton explains. "It can lead to a sprawl of data across those services and a challenge around consistency of user experience, along with multiple logins and identities."

Wolters Kluwer's Smith has seen the challenges of a smooth migration firsthand – and knows that it's easy to underestimate the challenges that new architectures present for staff.

"You're moving to a completely different environment and changing a lot of the ways you work," he explains. "A transformation like this tests out your staff. It's a significant architectural move and the reality is that some staff may need support."

Following a clearly delineated migration path that includes initiation, planning, delivery and closeout phases helps ensure that questions around time, cost, quality and risk are addressed.

A key part of ensuring a smooth transition is to engage business leaders throughout the rollout. In Wolters Kluwer's case, Smith worked with a steering group that consisted of key leaders from each business group. Fortnightly meetings ensured a hands-on approach that smoothed the migration.

"In this way, the migration was being driven by their needs as well as

9.PwC: Global State of Information Security Survey 2014

our own," Smith says. "By the time we're finished, all of our customer-facing components and most of our back-office pieces will be in the cloud.

"Our cloud provider is in a better position to deliver this than we are, and we're really driving it at the top level. The key is to have the right partner – someone with the experience and responsiveness and strength to get you there."

KEY QUESTIONS

- Do you have the technical and change management capabilities to ensure a smooth transition into the cloud?
- Have business leaders been engaged enough to open doors for technological change advocates?
- Do you have access to the right partners and specialists to move smoothly into the cloud?

7. TECHNOLOGY ADOPTION

Once the technological migration to cloud is taken care of, organisations face their biggest challenge: helping users learn not only how to use the environment, but how to optimise its use so they can fully realise the productivity benefits it offers.

Technology is often bought and installed, but without communication, training and delivery of genuine business value its benefits might not be realised. The key is to ensure that your staff are empowered to work anywhere they need to.

Poppy Moore, IT Infrastructure Transition Manager at property services firm DTZ, says the firm expects significant improvements in workplace flexibility from the cloud, looking towards the Optus Unified Communications-as-a-Service (UCaaS) offering as it undergoes a demerger that will split it from parent company UGL.

DTZ's 1,200 Australian employees operate from six offices across the country, making effective communications critical to its success. Moore believes the cloud-hosted communications service will be the best way to provide robust, flexible collaboration tools that will link regional employees with peers across the 26,000-strong DTZ network spanning 52 countries.

"We wanted something that aided mobility, but didn't want to focus our technical skills on managing the phone system; we wanted to focus them on other business initiatives," Moore explains. "When we looked at the cost comparison to housing the systems on-site, versus acquiring them as a cloud solution, we felt there would be benefits in doing that."

Each company embracing cloud-based solutions will go through a process of re-evaluation, planning, implementation and, with appropriate action, eventual success – and most will encounter obstacles along the way as they confront the challenges of reconciling legacy infrastructure with the different demands of cloud-based services.

Overcoming these challenges, and driving user adoption, enables consideration of the benefits of operational changes such as hot-desking – which supports staff working outside of the office – and activity-based working, which represents a significant functional shift away from conventional models.

Since employees can remain constantly connected through the central cloud-based platform, they can realise the benefits of those new models and, in so doing, save themselves time and energy. Over time, this should also save the company money, as reductions in space-based costing are matched by improvements in worker productivity.

KEY QUESTIONS

- Have you deployed (or could you deploy) a bring-your-own-device environment?
- To what degree can cloud-based services simplify the transition to flexible working?
- Are your business processes being revisited to ensure that employees' productivity is not being compromised by outdated procedures or policies?
- As part of your technology rollouts, do you also produce a communication, training and adoption plan?
- Are you required to measure the business impact of your technology purchases?

CONCLUSION

Effectively migrating to cloud-based collaboration services requires careful consideration of all the factors discussed in this paper. In nearly every environment, new questions are certain to arise as business cases are reviewed and tweaked, technical resources are allocated, leaders become involved, staff are trained, and business and technological leadership roles change.

By delegating the underlying technological infrastructure to a service provider such as Optus, organisations are free to spend less time worrying about technical minutiae in the short term, and more time helping the business grow in the long term.

KEY CONSIDERATIONS

- Businesses are moving to cloud for applications and services, including Unified Communications-as-a-Service and Contact Centre-as-a-Service.
- Benefits include a simpler opex model, a scalable common platform, ongoing access to the latest software features and updates, and reduced business risk.
- Moving to the cloud requires careful planning to ensure smooth migration and integration.
- A clear implementation methodology ensures every business and IT-related aspect is addressed, with deliverables repeatedly checked against expectations.
- Reaping the benefits of cloud services requires careful attention to training and empowering staff so they can make the most of the new technologies.