

## Pragmatic tradeoffs in enterprise adoption of public Cloud

by Dr Steve Hodgkinson, research director - public sector, Ovum Australia and New Zealand

Ovum predicts that the Asia-Pacific region will be the fastest growing public Cloud market, growing by over 30 per cent per year between 2011 and 2016. This 'radical externalisation' of ICT capabilities is met with serious concerns over corporate data sovereignty, security and privacy. However, Ovum believes that the perceptions of risks may have been overblown. The regulatory and security issues should be treated as business requirements to be met and risks to be mitigated, not as showstoppers of Cloud adoption. Risk mitigation comes from selecting a trusted Cloud provider who fears the 'wrath of the crowd' and resolves issues to avoid it. Nevertheless, Cloud providers must ensure they apply all the necessary security measures and also avoid the 'lock-in' threat by making it easy for enterprises to leave, should they want it.

*Dr Steve Hodgkinson is research director - public sector of Ovum's government practice in Australia and New Zealand. Prior to joining Ovum he was the Deputy CIO for the Victorian State Government in Melbourne, where he was responsible for e-government and IT strategy across the State Government's departments and agencies. He led a four-year programme of activity to establish the Office of the CIO and implement shared services and infrastructure consolidation initiatives.*



*Dr Hodgkinson has an in-depth knowledge of business and IT strategy, and experience with large public and private sector organisations in Europe and Australasia. He also founded and sold an e-commerce company. Dr Hodgkinson is a frequent commentator on the ICT (Information & Communication Technology) industry in Australia, with a focus on public sector ICT issues. He writes regular columns in a number of leading ICT magazines and is often invited to speak at conferences and at client workshops and events. He has a doctorate in Management Studies from the University of Oxford and a first class honours degree from the University of Otago in New Zealand.*

*Some recent examples of his relevant advisory engagements include assisting an Australian state government with independent assessment of vendor presentations during a large-scale tendering process for a managed desktop environment. Another engagement was briefings to a number of state government agencies on recent developments in the web 2.0 and enterprise 2.0 arenas and their implications for office worker productivity and collaboration in the public sector. He also conducted a market scan of manufacturers of operating systems, office automation and business utility software for an Australian state government - addressing the question 'Is there a viable alternative to Microsoft software for large scale enterprise office automation environments, and if so which vendors could be candidates to dislodge Microsoft from its position as the de facto standard for desktop software?'. He also reviewed a state government's enterprise licence agreement for IBM software (including Lotus office productivity products) and provided negotiation advice. He advised a state government agency on the leading enterprise web content management system vendors as a precursor to a public tendering process and investigated the implications, pros, cons and issues relating to migration from Lotus Notes to Microsoft Exchange.*

Enterprise use of public Cloud services is now widespread and growing around the Asia-Pacific region. However, many regulators and security authorities remain cautious due to concerns over data sovereignty, security and privacy of data in the public Cloud. Such concerns are holding back adoption, particularly in the financial and government sectors. Ovum's research reveals that early adopters of public Cloud services take a practical view of benefit/risk tradeoffs. Regulatory and security concerns are business requirements to be met, not showstoppers of Cloud adoption.

A useful addition to the enterprise ICT portfolio Organisations around the world, from small businesses through to large corporate and government enterprises, now rely on the public Cloud to support services ranging from niche ICT applications to mission-critical operations.

Ovum estimates that public Cloud services generated globally around US\$18.2 billion in revenue in 2011. The forecast is that this will grow by 30 per cent per year, exceeding US\$65 billion by 2016. The Asia-Pacific region is expected to comprise the fastest growing market for public Cloud services, with revenues forecasted to grow by 34 per cent per year from US \$2.9 billion in 2011 to US\$12.5 billion by 2016.

Software-as-a-service (SaaS) offerings comprise the most mature examples of public Cloud services from an enterprise perspective. Proof points of the widespread and growing adoption of SaaS services include:

- Salesforce has many thousands of customers across the region, comprising a mix of large corporate and government sector enterprises and SMB (*Small to Medium Business*) organisations. Use of Salesforce is steadily expanding beyond

its CRM (*Customer Relationship Management*) application into a wider range of apps and its broader platform-as-a-service offering.

- NetSuite also has thousands of customers, predominantly in the SMB sector, but also including subsidiaries of larger corporations that use NetSuite as a common financial reporting platform.
- Adoption of Google Apps and Microsoft's Online services is growing - leveraging initial email deployments into a broader range of collaboration and office productivity apps, particularly in the higher education sector.
- Other SaaS applications popular in the region include Microsoft Dynamics CRM, Oracle CRM On Demand, RightNow, SuccessFactors and Yammer. There are many hundreds of other niche SaaS applications in daily use.

Public Cloud services bring two main benefits, both attributable to the 'radical externalisation' of ICT capabilities beyond enterprise scale - into the Cloud. First, the public Cloud can offer

a more effective and efficient way to source selected ICT applications and infrastructure capabilities as-a-service. Second, it can offer a new way to accelerate participation in the rapidly evolving social networking and mobile solution ecosystems of the Internet age.

### Risk perceptions are becoming overblown

While enterprise adoption of public Cloud services is widespread, cautionary statements by regulators and security authorities of the theoretical risks of off-shore data storage in the public Cloud amplify risk perceptions. Statements about privacy risks and exposure to the US Patriot Act, for example, serve to heighten awareness of regulatory uncertainties and potential security and compliance issues - particularly in the government and financial sectors.

Cloud critics, some with vested interests in the status quo, are vocal to intensify risk perceptions further. On the other side of the argument, the safety assurances of public Cloud vendors tend to be discounted as marketing. At the same time, enterprises with hands-on experience of the public Cloud are relatively silent about their experiences due to perceived compliance sensitivities. The result, in Ovum's view, is that risk perceptions have become overblown.

### Wise use of the public Cloud is all about the right approach

To shed some light on the reality of how the Cloud feels in practice we interviewed executives in ten Australian corporate and government enterprises with hands-on experience of market leading public Cloud services. Discussions were intentionally 'off the record' in order to encourage open and frank discussion.

The results convey positive experiences. The executives we interviewed stated that the public Cloud has added value to their enterprise's ICT portfolio. Public Cloud services were typically not chosen to save costs. In most cases the service was selected because it was better and faster - even though some changes to information management practices were required. One of the most strongly valued benefits was iterative functional evolution. The Cloud service addressed user frustrations with the slow cycle of innovation of past ICT solutions as well as user expectations that modern Internet applications should be constantly evolving in terms of their functionality and support for innovations such as social networking and mobility.

Concerns over data security and regulatory compliance were taken seriously, but were not viewed as 'showstoppers' as long as careful thought is given to the categories of data that will be stored in the Cloud and to identifying specific risk factors and mitigations in process controls and contracts. Not all public Cloud services are equal in terms of their ability to meet enterprise reliability and security requirements, so the

biggest risk mitigation was the choice of a high quality enterprise-grade Cloud services provider.

Data sovereignty issues create an undercurrent of worry about off-shore data storage for some executives - although this was acknowledged as a justifiable benefit/risk tradeoff, as long as the potential risks were judiciously managed. In the medium term, a number of executives felt that a key emerging differentiator for public Cloud service providers would be the ability to provide robust encryption of data 'at rest' and choice about data centre location.

The executives interviewed had gone into the public Cloud 'with their eyes open' and were comfortable with the tradeoffs required in order to access the benefits provided by the Cloud services.

### Recommendations for enterprises

1. Approach Cloud computing from a strategic perspective

Public Cloud services are a radical externalisation of ICT capabilities that require some new tradeoffs - and a willingness to 'think outside the box'. Managing a shift in the balance of the tradeoffs is part of a strategic transformation of the enterprise's approach to ICT, not simply an expedient way to source a new point solution.

2. Acknowledge that scale matters for safety in the Cloud

Significant investments in technology, processes and people are required to build and sustain an enterprise-grade public Cloud service. Concerns over the fact that global public Cloud services providers will store data off-shore need to be balanced against the capacity that global scale brings to invest in service innovation, functionality, reliability and security. The primary concern should be the depth and quality of the overall service offering ... not simply the location of the data.

3. Don't compromise on enterprise-grade compliance requirements

The convenience of end-user adoption and low entry costs of public Cloud services are no excuse for lower standards of security and compliance. The biggest risk mitigation is the choice of a Cloud services provider capable of operationally and contractually meeting compliance requirements. Cloud services create both the imperative, and the opportunity, for enterprises to focus less on technology and software and more on the essentials of compliance - processes and information. Overall standards of security and compliance can be increased through Cloud adoption when it is combined with a renewed focus on process discipline and information categorisation and governance.

4. See beyond the contract and SLA (*Service Level Agreement*) to harness the power of the 'wrath of the crowd'

While a contract and a service level agreement are essential to reach an agreed basis for the commercial relationship, enterprises also

need to appreciate the importance of the 'wrath of the crowd' in public Cloud service relationships. The bigger the crowd the greater the wrath; that is, more pressure can be applied on the Cloud provider to prevent service issues and resolve them quickly. The fact that large numbers of customers share a common service means that there is 'safety in numbers', which is a significant change in the logic of power relationships in enterprise ICT procurement.

### 5. Rein in 'stealth' Cloud adoption

While it was fashionable a few years ago to admire the innovative energy of line-of-business executives who acted independently of the ICT department to acquire public Cloud services 'because they could', this behaviour is one of the drivers behind regulatory concerns. The reality is that ICT departments must rein in 'stealth' Cloud adoption and bring it under normal ICT governance arrangements. We can be sure that auditors and directors will pay increasing attention to this over the next year, so CIOs are recommended to get to the front line in order to be able to deal with issues proactively rather than in a crisis.

### Recommendations for vendors

1. Making the public Cloud safe and trusted for enterprise use is not optional

The rate of growth of the public Cloud market in the enterprise sector will be very much determined by the success of the major vendors in meeting enterprise reliability, security and compliance expectations. It is not enough for the public Cloud to offer superior functionality - it has to offer superior trust as well. The actual and perceived trustworthiness of individual public Cloud vendors will become a significant source of differentiation in the enterprise market.

The ability to efficiently encrypt data will be strongly valued by enterprise executives. As soon as this is technically, operationally and commercially feasible, it will be strongly recommended by regulators, and hence regarded as a prerequisite for the use of public Cloud services by auditors and company directors.

2. Find ways to develop peer-peer networks of customers and prospects

Public Cloud providers have much to gain and little to lose by encouraging networking and information sharing between customers and prospects. The rate of enterprise adoption of public Cloud services will be accelerated by more transparency around how data security and privacy concerns are overcome in practice to counterbalance the cautionary statements made by regulators.

3. Make it easy for customers to leave ... and ensure that they have no reasons to want to  
Concern over lock-in is somewhat over-hyped, but nonetheless is a recurring worry of executives. We recommend that public Cloud services providers make a virtue out of making it easy for customers to both subscribe to and terminate the service. Paradoxically, customers will be less anxious about adopting a public Cloud service if they are confident that they can leave at any time, taking all their data and erasing any trace of their use of the service. ●