The convergence of mobile, cloud computing and the Internet of Things (IoT) heralds a new era of hyper connectivity, and with it, high expectations from students, staff and faculty for anywhere, anytime Internet availability and data sharing in real time.

Moving services to the cloud can deliver significant infrastructure benefits and cost efficiencies to help the education sector meet these new expectations, but these opportunities come with risks that are sometimes overlooked in the rush to join the crowd in the cloud.

It’s important to consider the risks, as well as the benefits, when making decisions around outsourcing IT services to the cloud. Rethinking business continuity and disaster recovery plans is vital for ensuring that any investment in cloud services will meet the service delivery expectation goals of institutions, now and into the future.

**How has the rise of cloud computing impacted IT Services?**

The traditional custodians of IT Services (ITS) have taken great steps towards standardisation, repeatable performance and risk mitigation for highly available cost-effective service delivery. They have achieved this by building resiliency into infrastructure designs, coupled with best practice operational processes for managing infrastructure or service failure.

This traditional paradigm has served institutions well, until today, when disruption from cloud service providers means that it is no longer acceptable to follow standard repeatable methods that involve long lead-time and personalisation service-based costs. Cloud-based services hosted off campus offer flexibility, with easy payment options for immediate results, and are leading user communities to bypass ITS without the recognition of costs and risks related to data security, data ownership, scalability and resiliency.

Cloud has accentuated the importance of the entire data network as a vital piece of infrastructure, acting as the glue between connected devices on campus and data, applications and services hosted locally or in the cloud. Today’s university campuses support thousands of researchers, students and staff who expect to auto-connect multiple mobile devices to wireless networks, and have information at their fingertips. Digital signage is appearing across campus precincts, combined with information to mobile apps, this too offers an unprecedented flexible communication opportunity that also relies on the network.
Cloud: what are the benefits?

In layman’s terms, cloud computing means that campuses can lease data centre compute, storage and networking (physical or virtual) resources in the form of services as part of an online self-help service catalogue, instead of managing these resources in-house on campus.

Moving services off-site offers the advantages of highly available and resilient network service connectivity from cloud service providers who can demonstrate best practice operations and support levels.

Third party providers generally offer better physical and online security, access to more resilient and scalable capacity and 24x7 monitoring and support than the typical on-campus set-up, because it is their core business. Moving to the cloud can provide greater resiliency by removing total dependency on the campus network for service access, and at peak utilisation times, such as enrolment, assignment submission and exam results times, supporting the elasticity to provision extra resources automatically.

What are some of the risks?

On the flip side, cloud services can become expensive depending on how the resources are utilised. Costs tend to be itemised and payable on a pay-as-you-use model. Careful modeling of data and services that require high availability and extra resources at peak times is recommended. Without that analysis, potential cloud economies of scale may not be realised.

Choosing a decentralised approach to service delivery may also be unsustainable and risky, especially at a time when universities are expected to operate on lower operational budgets, or when ITS may be perceived as non-core activity (i.e. not direct revenue generating).

Undertaking a medium to large-scale realistic disaster test scenario involving IT Services of half a day or more, in this case, may be viewed as low priority, increasing the risk factor.

How to mitigate risk

Business continuity professionals face a challenge and an opportunity to optimize an institution’s approaches to outsourcing IT services to third parties.

Consider the impact a real disaster can have on business operations: disruption, data loss and data restoration efforts, and also reputational damage and the prospect of higher insurance premiums for many years thereafter? Disruption could be as simple as police cordoning off an area of the campus that includes the data centre, restricting access for a number of days, for example. It makes sense to consult with emergency services for advice and to build their procedures into disaster recovery plans.

When considering migration to the cloud, the network and network security become key to service continuity. Cyber Security attacks such as Distributed Denial of Service (DDoS) on compromised machines can impact server computation load or network connectivity, impacting services delivery and cost. It remains unclear whether on-campus or cloud is better, the former may offer greater direct control, whilst the latter may offer greater resources for defense.

Agreeing to favourable contract terms with third parties can help mitigate risk in the form of service level protection and even financial penalties. Should a third party provider experience issues, penalties may be less of an issue than the loss of your critical business operations and reputation.

Any decisions to move online services to the cloud should be based on a comprehensive risk assessment and a cost of ownership comparison based on forecasted growth. Although factors other than costs may be drivers, this would at least address financial impacts.

Should a number of services move to the same cloud provider (either in an orchestrated or uncoordinated way), consider that risk may simply be transferred to reappear elsewhere.

Planning for when disaster strikes

In the event of a disaster, damage assessment teams need to be confident that existing communications can facilitate coordination. Some institutions assume Internet connectivity will continue and be supported by ITS and that if Internet fails, the fallback is 4G mobile services.

Disasters have a tendency to overload mobile phone towers for voice and data services. Mobile may be an unreliable means of communication for coordinating with emergency services for work-related incident management.

It is vital to have a plan A, B and C for enabling communications for crisis command.

Good old fashioned printed copies and a battle box at an agreed offsite location such as a hotel is recommended. Satellite phones for key staff and plain old telephones in data centres to coordinate any safe shutdown and removal of equipment, where it is safe to do so, is also an important consideration. Having a ready and trained incident management team and sub teams that test scenarios several times per year are key to the success of any technology continuity plan.
8 tips for improving your risk profile in a cloudy environment

Here are some tips to improve your risk profile by adopting a range of business continuity suggestions and provisions:

1. **Proactively design with resiliency in mind**
   Carefully select resiliency features for infrastructure and setup at alternative sites.

2. **Think about when an IT operational issue becomes a disaster or a ‘Disaster’ is actually only an operational issue**
   Working through that detail is likely to save you from the costs of mobilising teams too quickly or not reacting quickly enough, and losing value time to respond.

3. **Explore and test your crisis management and crisis command management capability**
   Is it taking advantage of the latest cost effective communications systems available?

4. **Test IT Disaster Plans with IT Services**
   Move beyond isolated incidents to connected incidents and definitely explore an inaccessible data centre scenario in detail. Bring in external IT experts to assess your IT effectiveness and impact.

5. **Make sure you know your last data point (when you last backed up your data)**
   Be clear on how long you can continue with manual workarounds before access to that data becomes imperative to maintain your business operations.

6. **Test cloud service provider disaster recovery plans; assess their SLAs**
   Consider what would happen if the Cloud Provider went offline or went out of business, what are the impacts and options for your business?

7. **Seek out like-minded partners, even competitors, for sharing infrastructure in the event of a disaster**
   An in-principle agreement costs nothing but can provide you with options when you most need it.

8. **Address the loss of key people**
   Many institutions do have experienced staff with lots of knowledge buried in their heads or rely on outside consultants and experts. Encouraging these busy people to participate in business continuity tests, even as the observer in the role, to encourage greater staff rotation and succession planning can lower business continuity risks.

**Summary**

Cloud computing presents many opportunities for streamlining IT service delivery in a time where IT Services managers need to do more with less. Managing the risks associated with outsourcing IT services to the cloud is vital. Take steps to build robust disaster recovery plans to safeguard business continuity.

Engage with key influencers and stakeholders, share resources and seek out what resonates best within your institution. Prioritise areas of concern and offer a balanced approach to communicating risks and impacts (glass half empty) and creating opportunities for change and innovation (glass half full).

**About the Author**

James Sankar established AARNet’s Enterprise Services team of independent consulting engineers that supplies IT consultancy services exclusively for AARNet customers. The team provides on-demand engineer and project management resources to assist with service delivery, data protection and business continuity.

James Sankar
Director, Enterprise Services
AARNet Pty Ltd
james.sankar@aarnet.edu.au

*Opinions expressed in this white paper may change over time.*