Meeting the Challenges of the Cloud in Post-Secondary Education

2012

Contact North | Contact Nord
Ontario's Distance Education & Training Network
Le réseau d'éducation et de formation à distance de l'Ontario

www.contactnorth.ca | www.contactnord.ca

Cloud computing challenges post-secondary education's habit of supplying our own technology needs.

Executive Summary

Information technology is being reshaped by techniques that make it easier to consume computing power without owning or managing the infrastructure that provides it. By replacing assets like servers and data centres with services delivered over the Internet, cloud computing challenges post-secondary education's habit of supplying our own technology needs with resources that our institutions own and operate on campus. It not only provides our leaders and IT administrators with new ownership alternatives, but opens new opportunities for collaboration, and empowers local users to make their own technology choices.

In its essentials, cloud computing is:

- On-demand: cloud services are just "there" and available for use, and billed on a usage basis rather than being owned or leased;
- Shared: many customers use the same resources via networks, feeding economies of scale;
- Configurable: individual customer services can be flexibly configured and managed with minimal or no expert intervention; and
- Elastic: capacity and service use can grow on demand, then shrink or disappear when demand drops or needs have been satisfied.

Cloud services available in the marketplace range all the way from raw computing power chiefly consumed by technical users to refined applications directly useable by students, faculty members, and staff.

Meeting the Challenges of Cloud Computing

Cloud computing is a breakthrough technology not because it delivers services from remote computers—which has been possible for many years--but because it makes services easier to use, more abundant, and more cost-effective.Just the same, by shifting the balance of IT power from the institution toward external resources, it presents legal, ethical, technical, business, and cultural challenges that we consider in this paper.

Challenges post-secondary institutions will confront as they move to realize the benefits of the cloud include:

1. Understanding an immature marketplace. Today only a small percentage of global IT spending goes to public cloud services, and the marketplace is full of new companies and unproven cloud solutions. But cloud spending is growing at five times the rate of overall IT spending, and cloud products will mature over the next two to five years. Institutions can take advantage of cloud opportunities while protecting themselves fromundue risk by using the cloud for non-core and testbed projects; by employing it in relatively well-proven domains like email and office productivity tools; and by assuming early-adopter risks where the strategic rewards are potentially high.

2. Solving the cost equation. Cloud computing shows real promise for achieving IT cost savings in certain circumstances, but costs can be hard to ascertain and the economics of the cloud still aren't well understood. Institutions need to be skeptical about vendor claims, develop the skills to ascertain the total cost of cloud and premises-based solutions over their full lifecycle, and be receptive to non-cost benefits of the cloud, including greater agility and the ability to launch new initiatives more quickly.

3. Preserving data security and integrity. Cloud computing's reliance on remote, shared, "multi-tenant" infrastructure and its removal of business processes from direct institutional supervision raise real security concerns, but these have to be balanced against the risks confronting on-premises systems. Institutions can limit risk by restricting cloud use to low-sensitivity applications or by participating in education-specific private or community clouds. For more sensitive applications, it's important to thoroughly assess cloud provider security practices as well as your own environment's security profile. Third-party assessments can be helpful in both areas.

4. Privacy and regulatory compliance. Cloud service providers don't necessarily make allowances for post-secondary education's regulatory needs, and cloud-based data can easily flow across borders. Institutions must ensure that Canadian federal and provincial privacy requirements are reflected in contract terms, and they should thoroughly investigate how and where cloud services operate. Private or community clouds operating exclusively in Canada are a potential additional resource to consider.

5. Getting it all to work together. When assessing cloud service costs, be sure to take into account both the costs and the benefits related to getting different systems to work together smoothly. Robust systems for identifying users to internal and external online resources are a powerful tool for taking down barriers, as well as an important security safeguard.

6. Avoiding lock-in.Be sure you understand the mechanics of switching away from any critical external service, and identify alternative providers and/or scope out what it takes to deliver the service internally. Maintain an independent capability to assess technology, manage it, and integrate its different functions.

7. Preparing the organization. In a cloud-oriented environment, users will have to be educated to choose cloud services wisely, while technology organization will be less dedicated to managing data centres and deploying enterprise systems, and more dedicated to user education, integration, and providing safe pathways to external resources.

Opportunity and Challenge in the Cloud

For the next few years, the cloud will be a risky place for post-secondary education, but the risks are manageable and outweighed by the opportunities. The greatest risk imaginable is to wait for every aspect of the cloud phenomenon to mature, while somebody else masters its challenges and earns its rewards.

New technologies make it easier to consume computing power without owning or managing the infrastructure that provides it.

How can the cloud serve post-secondary education's needs?

- A computer science instructor wants her students to solve a certain design problem in different technology environments. Instead of configuring local servers, she uses platform-as-a-service tools to make the appropriate environments available, then releases them when the assignment is over.
- An institution's IT organization counts dozens of e-mail systems on campus. Replacing these with a unified on-campus system will improve service, but will also require major up-front hardware and software investments. Instead, the institution turns to a cloud-based system that provides email, calendaring, and office productivity applications in the form of software as a service.
- A research lab needs to convert real-time experimental data into normalized formats. Researchers use commercial infrastructure-as-a-service to set up and test the data processing application, then ramp up their computing power as the data streams in. When the experiment is over, they release the unneeded processing power.
- A university's new branch campus in Shanghai needs a room scheduling system, but the mother campus system isn't designed for global operations, and installing a local system would take too long. The new campus turns to a software-as-a-service solution that becomes functional as soon as building and scheduling information can be uploaded.

Introduction

Once again, information technology is re-inventing itself. At the crux of the change is a collection of technologies that make it easier to consume computing power without owning or managing the infrastructure that provides it.

With just an Internet-connected PC or mobile device and simple software like a browser or app, users can now set up remote computing environments as big or small as they need, and adjust usage up or down when needs change. They candeploy their own applications on distant technology platforms, or do business using third-party applications they never have to buy, install, or update. Or, as millions of consumers already do, they can draw on libraries of music, video, and literature, anywhere and at any time, without owning or even handling any physical media.Technology capabilities made available in this way are known as services,and the galaxy of services available over the Internet is increasingly known as “the cloud.”

The key value proposition of the cloud is to useservices to take the place of assets—the streamed video instead of the DVD, the functionality of the payroll system without the servers and data centre racks it runs on. The cloud’s services are available anywhere a network connection can be found, liberating users from relying ona particular machine’s installed applications and storage.

Much of what the cloud delivers is enabled by cloud computing, a set of technologies that pool computing power and deliver it to remote users in very flexible ways. Reduced to essentials, cloud computing is:

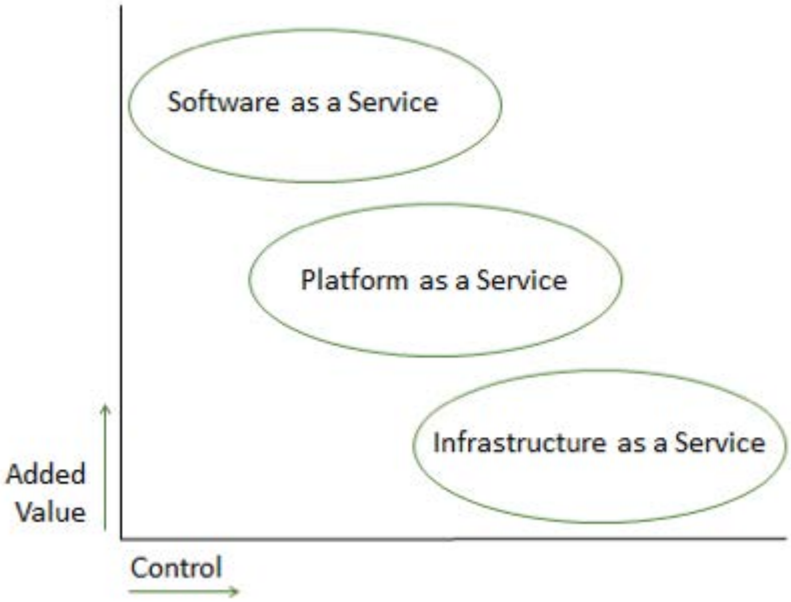
- Available on-demand: from the user’s standpoint cloud services are just “there” and ready for use, billed on a usage basis rather than being owned or leased;
- Shared: many customers use the same resources via networks, permitting economies of scale;
- Configurable: individual customer services can be flexibly configured and managed with littleor no expert intervention; and
- Elastic: capacity and service use can grow on demand, then shrink or disappear when demand drops or needs are satisfied. This departs markedly from the current practice of building “just-in-case” IT resources to accommodate growing institutional demands.

Cloud computing is a breakthrough technology because it makes remote services easier to use, more abundant, and more cost-effective.

Cloud computing helps hide complexities from end users, giving them just the services they want without extraneous effort. Infrastructure as a service(IaaS)delivers on-demand, elastic access to basic hardware like servers and storage. Platform as a service(PaaS)provides, in addition to basic hardware and storage, technical components such as programming languages or other tools that make it easier for users to create and deploytheir own applications.. And when users want the functionality of ready-to-use applications like e-mail or payroll, software as a service(SaaS) can deliver it.

Cloud services, then, range all the way from raw computing power chiefly consumed by technical users to refined applications directly useable by students, faculty members, and staff. As a rule, cloud services lower in the value chain offer more control but leave more for the user to manage, while those farther up are more constricted but easier to use (see Figure 1).

Figure 1. Cloud Services Models



Cloud computing is a breakthrough technology not because it delivers services from remote computers—whichhas been possible for many years--but because it makes services easier to use, more abundant, and more cost-effective. It is in many ways the evolution of earlierIT outsourcing methodssuch as software hosting, in which a software application is licensed to an institution and runs on its own server but is operated and maintained by an external hosting vendor. Many variations on this theme coexist today with emerging cloud solutions, and have valuable lessons to offer about managing the cloud environment.

Like any new technology, cloud computing will go through some bumpy patches, and will surprise us with both failed promises and unexpected successes.It has attracted levels of hype not seen since the days of dot-com mania. Our purpose in this paper is to help education leaders understand and navigate through the risks and challenges, so that they can realize the cloud’s revolutionary potential.

The cloud challenges post-secondary education’s habit of supplying its technology needs with premises-based, institutionally owned and operated resources.

Why take on the cloud’s challenges?

A companion whitepaper, Cloud Computing Opportunities for Post- Secondary Education, outlines the cloud’s potential to:

- reduce IT capital expenditures,
- help institutions aggregate demand and share services,
- improve institutional agility,
- make IT more energy-efficient,
- expand educational services globally, and
- enrich learning through an emerging ecosystem of cloud-based educational resources.

Meeting the Challenges of Cloud Computing

Cloud computing’s impact on post-secondary education will take time to unfold. But one key implication is abundantly clear: the cloudchallenges post-secondary education’s habit of supplying its own technology needs with resources that the institutions own and operate on campus. It not only provides leaders and IT administrators with new ownership alternatives, but opens new opportunities for collaboration, and empowers local users to make their own technology choices. We also need think deeply about the clear fact that cloud-based services are already transforming many consumer markets, with major implications for all information industries.

Just the same, the cloud can’t solve every problem, and by shifting the balance of IT power from the institution toward external resources, it presents legal, ethical, technical, business, and cultural challenges. Some of these challenges arise from the way cloud resources work—or don’t work—and from the uncertainties of an emergent marketplace. Others arise when business processes move away from direct institutional supervision while accountability stays at home. Some challenges flow from trying to map the concerns of post-secondary education on to resources that are designed to serve as wide a range of customers as possible. And some come from the need to rebalance skill portfolios, educate staff about good cloud computing practices, and generally prepare our institutions for the idea that we can’t—and shouldn’t—do everything for ourselves.

In the following sections, we look at some particularly important challenges the cloud presents, and suggest ways of meeting them.

Challenge 1: Understanding an Immature Marketplace

If one statistic best underscores the fact that cloud computing remains an emergent technology, it's this: according to the research firm Gartner, of the $2.3 trillion enterprises spent on IT globally in 2011, only about 3% was spent on public cloud services[1]. Adding spending on "private" clouds operated by organizations for their own use would undoubtedly yield a larger figure, but even so, cloud spending is clearly dwarfed by the traditional model of enterprise-owned data centres and non-cloud providers.

A look around the vendor landscape further reveals a marketplace in its early stages. Though giant technology companies like Google, Amazon, Microsoft, and IBM are major players in cloud services, the vast majority of their revenues come from other lines of business. The largest of the "pure play" enterprise software-as-a-service vendors, Salesforce.com, had revenues of $1.7 billion in 2011, a small fraction of its more traditional rivals Oracle and SAP. The cloud has introduced a lot of new names into the staid world of business software, among them SuccessFactors, a software-as-a-service human resources company recently acquired by SAP, and Workday, another HR SaaS startup that has identified higher education as a key target industry.On the other hand, some of the product lines of greatest interest to higher education, like the administrative suites from Oracle/PeopleSoft and Ellucianlack pure cloud delivery options, though they are available in hosted solutions with some cloud-like features.

If cloud revenues make up such a small niche of the massive IT marketplace and many of the new players and products are unproven, why all the excitement? For one thing, that "tiny" 3% share of worldwide revenues defines a $74 billion marketplace—hardly an insignificant opportunity. More importantly, Gartner and other research firms estimate that the cloud's share of sales is growing at five times the rate of the IT market overall, and will do so through 2015.And cloud computing's impact on global computing is already being felt, with much more to come. According to Cisco Inc., though the server workloads carried by traditional data centres exceeded those in cloud data centres by four to one in 2011, the balance will tip by 2014, and in 2015 cloud data centres will handle 57% of all server workloads[2].

Research firms estimate that the cloud's share of global sales is growing at five times the rate of the IT market overall.

As cloud technologies and vendors mature over the next two to five years, post-secondary educationobservers will undoubtedly see growing pains including vendor failures and acquisitions, evolving business models, product flops and ongoing hype. Institutions can protect themselves from undue risk, while exploiting the possibilities of the cloud,by adopting some classic techniques for making decisions about volatile technologies:

[1] « Gartner Says Worldwide IT Spending to Reach $2.7 Trillion in 2012 », dans le site Web à l'adresse http://www.gartner.com/it/page.jsp?id=1824919.

[2] Cisco Inc., Cisco Global Cloud Index: Forecast and Methodology, 2010-2015. [En ligne] dans le site Web à l'adresse http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Nuage_Index_White_Paper.pdf.

1. Use the cloud as a sandbox. The cloud's on-demand availability and freedom from capital commitments make it an ideal test bed for prototyping, meeting unexpected demands, and getting entrepreneurial ventures in motion. Experimenting with smaller non-core systems that don't expose vital institutional data and don't require conversion from entrenched legacy systems is a good way to encourage creative initiatives with minimum risk and cost. In the meantime, your institution will build experience, and discover where cloud solutions work and where they don't.

2. Follow the leaders. Cloud computing is not uniformly immature; it already has its success stories, and there are some areas where it can be called mainstream, or nearly so. Over 40% of US institutions of higher education and three-quarters of those in Australia and New Zealand have adopted the cloud-based e-mail and office productivity suites from Google, Microsoft, and other vendors. Cloud-based learning management systems is another area of relatively established practice. While not without their complications, cloud services like these are well removed from the pioneer stage, as Canadian adopters of cloud e-mail/office suites like the University of Alberta and the University of Toronto have shown.

3. For the right strategic reasons, consider the big bet.There can be good reasons to embrace a technology in its formative stages: to realize a key strategic ambition, differentiate the institution competitively, or leapfrog from an obsolete to a cutting-edge practice. Ground-floor development partners may be able to influence a new product's direction and secure good contract terms. Workday's signing of a core group of high-profile, early-adopting US institutions is a cloud-era reprise ofearlier generations of administrative system development. But never choose this option just because it seems like a moneysaver or "looks progressive." The leading edge is often called the bleeding edge for a reason.

Does cloud computing save money? The best answer probably is "it depends."

Challenge 2: Solving the Cost Equation

Compared to premises-based computing, cloud computing offers an entirely different model for acquiring technology. Cloud users don't buy hardware up front and set it up in a data centre. If they're using SaaS services they don't purchase perpetual software licenses and don't have to have staff on hand to update software. Because cloud services are adjustably "elastic," users don't have to maintain excesscapacity to meet occasional spikes in demand—they just dial capacity up and down as needed.Public cloud services are also better able than institutional data centres to exploit economies of scale.

So cloud services clearly allow our institutions to transform capital expenditures into more flexible, less committed operational expenditures, and they have the potential to get a unit of work done cheaper. But does cloud computing actually save money in the long run? This remains a controversial matter. At this stage of relative immaturity—and maybe permanently--the best answer probably is “it depends.”

Often the best reasons for using a cloud solution are to improve focus on core services, to get an initiative up and running sooner, or to obtain flexible capacity.

There certainly are reasons to believe that cloud computing can save money. One consulting firm, looking at US federal government computing environments, estimated that moving from traditional to cloud computing could shave up to 65% off of system lifecycle costs and achieve payback within three to four years[3]. Another analysis suggests that for a typical systemconfiguration, a cloud solution will save 29% on infrastructure costs compared to in-house IT and 18% off of a managed services approach (in which the organization owns the hardware but hires a third party to operate and manage it). Savings can be greater still where short-term peak loads are dramatically greater than standard loads—not an unusual situation; think of students registering for courses at the last minute a few times a year—because in a non-cloud environment these situations require carrying more stretch capacity[4]. A recent global survey of companies using cloud services found that 82% reported cost savings through cloud projects, though the savings were usually modest[5].

This is, however, a topic in which details can bedevil a clear outcome. Not all applications or business services, for example, are equally good candidates for deploying in the cloud. Cloud options are often best with new “greenfield” applications, thanks to their new technology and to the switching costs associated with older systems. Fully and accurately estimating the operating costs of premises-based systems in order to make a cost comparison with cloud services is notoriously hard to do,since local systems often rely on shared infrastructure and staff resources whose costs aren’t easily allocated. Infrastructure and staff costs don’t always drop even when cloud services remove loads from them, owing to fixed overhead costs and inflexible personnel policies.

Cloud prices, for their part, must be examined carefully. Service providers will naturally try to capture some of the cloud’s cost advantages for themselves by charging a “utility premium.” It’s also necessary to ensure that an apples-to-apples comparison is being made. Does a cheaper apparent cost per unit of work, for example, include the backup and disaster recovery services that an institutional IT shop normally provides? Will the institution have to invest in beefier networks to ensure acceptable response times?

Many analysts suggest that, while cost savings are possible in particular circumstances, often the best reasons for using a cloud solution are to improve focus on core services, to get a business initiative up and running sooner, or to obtain flexible capacity that renders “just in case” premises-based capacity unnecessary. One 2011 survey of IT professionals found that cost savings was only rated third among eight different motivators for using cloud resources; elasticity (adjustable capacity) and speed to deploy ranked ahead[6].

[3] Booz Allen Hamilton, The Economics of Cloud Computing, http://www.boozallen.com/media/file/Economics-of-Cloud-Computing-fact-sheet.pdf.

[4] George Reese, “The Economics of Cloud Computing” (O’Reilly Community), http://broadcast.oreilly.com/2008/10/the-economics-of-cloud-c.html.

[5] CSC Inc., CSC Cloud Usage Index (2011), http://assets1.csc.com/ newsroom/downloads/CSC_Cloud_Usage_Index_Report.pdf.

[6] Bitcurrent, Bitcurrent Cloud Computing Survey 2011, http://www.bitcurrent.com/ download/cloud-computing-survey-2011/.

These ancillary reasons for adopting the cloud can, of course, have beneficial cost and revenue effects of their own. Key advice for institutions examining the cost dimensions of the cloud are:

1. Be skeptical.Don't take vendor claims about cloud cost savings at face value.

2. Measure. Develop the capacity to measure the full spectrum of IT costs in both on-premises and cloud scenarios, preferably using methodologies like Total Cost of Ownership that consider costs holistically across a full system lifecycle.
3. Be flexible.Consider cloud advantages beyond cost savings, including those that improve institutional agility and lower barriers to new initiatives.

Challenge 3: Preserving Data Security and Integrity

The cloud raises legitimate security concerns, but they have to be balanced against the risks confronting the familiar institutional data centre.

No issue casts a longer shadow on cloud services than putting institutional and personal data on machines controlled by a third party. While this concern has always dogged IT outsourcing, certain characteristics of cloud computing have amplified it. Cloud environments rely heavily on "multi-tenancy," the sharing of resources by multiple customers. Multi-tenancy helps achieve economies of scale, but its importance goes beyond that. It enables the smooth adjustment of computing capacity as differentcloud customer loads surge and fall, and it facilitatesthe usage-based billing and easy self-provisioning features that are among the attractions of cloud environments.

Useful and even critical as it is, multi-tenancy does raise security concerns. For example, clouds use virtualization software that can run many virtual (emulated) machines per single physical machine. An intruder who penetrates the virtualizing "layer" that controls this process can in principle gain access to all the virtual servers running under that layer.

Likewise, software-as-a-service products typically use a single software instance to process work for many customers, and store the data for all those customers in the same database. (Workday and Salesforce.com work this way.)By contrast, in traditional premises-based computing and in some non-cloud forms of IT hosting, anorganization has exclusive use of its software and database. Again, in principle, someone with malicious intent—say, a cloud service customer breaking through the "walls" that separate different customer accounts--could access data for many organizations. There is also a theoretical potential for one customer's data to be inadvertently exposed to another's view, or for data to get corrupted from cross-processing. While public cloud providers have many engineering and policy safeguards against the dangers of multi-tenancy, including the encryption of stored customer data, they have also proved reluctant so far to accept liability for security breaches.

These dangers have to be balanced against the security risks confronting the familiar institutional data centre. Security companies routinely report that most of the customers they audit have potentially serious security weaknesses. Post-secondaryinstitutions are especially vulnerable, for assorted reasons: the distributed nature of authority and budgets, the many decentralized points where computing and networking takes place, and the general ethic of openness. Security expertise is expensive and stretched thin, and often has spotty authority over computing outside the central IT organization.

Cloud service providers operating at large scale can afford to spread security costs over a larger customer base and can monitor environments more consistently than anindividual university or college. As one writer puts it, "in theory, a single house with a fence around it is much more secure than an apartment in a block shared with many other households. In practice, the householders in the apartment block will pool the cost of having a porter on duty 24×7 to control access to the building."[7].

Institutions will have to examine the security aspects of the cloud just as they consider its financial and technical advantages.

In addition, the heavy redundancy built into cloud environments makes it easier to quickly shift processing to a ready standby if a certain server is compromised or failing. Their professionally administered servers are almost certainly better maintained with software patches and other security practices than machines outside the central IT core at most universities and colleges, and perhaps better than some in the centre. It's important to note, however, that cloud computing doesn't always mean service providers do this work: a customer settingup servers through infrastructure-as-a-service may be just as responsible for keeping security patches up to date as if he or she was working with premises-based machines.

In short, there aren't many absolutes in the security choice between cloud and premises-based IT environments. Institutions will have to examine the security aspects of the cloud just as they consider its financial and technical advantagescompared to other alternatives. Some key considerations to keep in mind:

1. Limit the risk.Institutions wishing to minimize exposure can limit use of cloud services to non-core and tactical applications, rather than strategic, must-have applications loaded with sensitive data. Another lower-risk use of cloud services is for development and testing purposes.

2. Probe provider security practices.When assessing cloud providers, thoroughly investigate their documented security practices, staffing policies (such as background checks for employees and staff certifications), security performance metrics, controls for separating customer accounts and data, and business continuity plans.

[7] Phil Wainewright, « Security Risks of Multi-Tenancy ». [En ligne] dans le site Web à l'adresse http://www.zdnet.com/ blog/saas/security-risks-of-multi-tenancy/1007.

3. Consider private or community clouds. Increasingly, national and regional networking organizations and other post-secondary education associations are experimenting with private clouds open only to colleges and universities. An institution with sufficient demand might also justify building its own cloud computing infrastructure. Though these solutions won’t enjoy the economies of scale of big public providers, and can’t promise perfect security, they narrow the range of “tenants” in the cloud environment and may be more sensitive to specific educational or regulatory needs.

4. Look in the mirror.Understand your own environment’s security profile through formal risk assessments and audits.

5. Get outside help. Consider retaining a third-party assessment firm to validate cloud service provider claims and to perform a reality check of your own institution’s security profile.

Challenge 4: Privacy and Regulatory Compliance

Like their natural cousins in the sky, technology clouds readily cross national and other jurisdictions. Not only can cloud server farms be half a world away from their customers, but they can change location without notice, and may make use of resources in different locations. Cloud providers may be tight-lipped about exactly where their servers are located. Users, meanwhile, are bound by laws with very literal and unchanging jurisdictional boundaries.

A particular concern for Canadian institutions is adhering to federal and provincial laws protecting personal information.

Moving to cloud-based student e-mail at the University of Toronto

Students communicate personal information via e-mail. The University of Toronto carefully addressed how best to protect privacy as it considered using the cloud-based Microsoft Live@edu email and collaboration service for its students.
Recognizing the ground-breaking work of the Ontario Information and Privacy Commissioner’s Privacy by Design (PbD) framework, the university developed a privacy impact assessment based on the PbD’sseven foundational principles. The university also carried out a threat risk assessment.

University officials communicated openly with the university community about the Microsoft service and its features and risks. The university negotiated contract terms consistent with Ontario law and permitted students to opt out of the service if they desired.

This approach was a success. After rollout to nearly 30,000 students, opt outs are below one percent.

Information about the Privacy by Design framework may be found at http://privacybydesign.ca/. Nor are geographic boundaries the only kind that complicates life in the cloud. Because cloud services are designed to service as wide a range of customers as possible, they frequently offer generic functions and contract terms without distinguishing between the needs of different industries and professions. Financial, medical, and educational data subject to dramatically different regulations may all be treated alike.

A particular concern for Canadian institutions is adhering to federal and provincial laws protectingpersonal information.Prompted in part by fears of foreign surveillance stimulated by the USA Patriot Act, two provinces, British Columbia and Nova Scotia, prohibit public entities from storing personal information outside of Canada. No other province does so, nor does the federal Privacy Act that governs the privacy protection responsibilities of public sector bodies[8]. But both provincial and federal laws do specify certain privacy protections, and organizations remain responsible for them when using external service providers.These protections typically include requiring consent for the collection, use, and disclosure of personal information, limiting its use to the purposes it was collected for, limited access and segregation of duties among those handling it, and notification in the case of information breach. Institutions contemplating cloud services that involve protected or sensitive information, particularly if they may cross national boundaries (and they probably will if they make use of big U.S.-based services) should ensure that RFPs and contracts explicitly specify such requirements.

Uncertainty about what happens when clouds drift across different jurisdictions is one aspect of the general immaturity of cloud solutions and cloud management.Case law, international negotiations, administrative experience, and evolving technology will probably help clarify the situation over the next few years, but in the meantime institutions will have to proceed carefully. They can:

1. Limit the risk.For reasons similar to those involved in cloud security, institutions may wish to limit cloud initiatives to projects that don’t involve sensitive data or regulated processes.

2. Look to the community. Defining a regulation-friendly environment and avoiding the complications of transborder data movements are among the best reasons to explore private or community cloud possibilities.

3. Find out the how, who, and where.When considering cloud solutions and vendors, be sure to have a thorough understanding of who is involved in delivering the service (including the service provider’s own contractors and providers), where processing and data storage take place, and how much access the service provider has to your data.

[8] Law Office of Kris Klein, Applying Canadian Privacy Law to Tran border Flows of Personal Information from Canada to the United States: A Clarification. [En ligne] dans le site Web à l’adresse http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Clarification%20Statement%20-%20Transborder%20flow%20of%20personal%20information.pdf/$file/Clarification%20Statement%20-%20Transborder%20flow%20of%20personal%20information.pdf.

4. Align law and contract.Work with institutional counsel and the service provider to ensure that cloud services contracts meet federal and provincial regulations, and develop a clear understanding of the provider's own obligations to respond to searches and other government demands in their own jurisdiction.

5. Communicate.If considering trans-border services, recognize that your institution's community may have norms and expectations beyond those specified in law, and be open about the nature and risks of services that affect them.

Integrating different systems and data stores is vital to efficiency and getting full value from information.

Challenge 5: Getting It All to Work Together

When IT professionals think about purchasing a new product, they don't just look at its functions and features. They're also interested in how well it plugs into the institution's complicated, interlocking environment of systems. While some services stand more or less on their own, others are intimately related to systems using the same data or performing related functions. Will the timekeeping systemfeed the payroll system data it can use? Can a student logging into the learning management system access the online library catalogue without entering a different account and password? Can amanagementreporting application read the transaction data maintained by the student system?

Integrating different systems and data stores is vital to operating efficiently and getting full value from information. In poorly integrated environments, data captured for one purpose is maddeningly unavailable for another, equally valid one. Managers can't answer simple questions abouttheir departments' performance and staff waste time trying to reconcile half a dozen systems' slightly different definitions of basic terms like "student" or "full-time." Everybody struggles with too many accounts and passwords.

Systems integration is notoriously challenging, but CIOs know that certain techniques can make it easier. They may prefer to buy as much as possible from a given vendor on the expectation that one vendor's products will work together better. They may deploy "middleware" products that help pass information between different systems, and favourproducts that use standardized ways of representing data and rules,so that program A can accept input from program B without knowing anything about B's internal workings. They especially like "open" standards that aren't controlled by a single company. They also know that well-designed identity management—the technologies and processes people use to identify themselves and gain access to systems—is a powerful tool for removing the barriers between systems, as well as an important security safeguard.

At least in the short run, cloud servicesmay prove difficult to integrate into institutional environments and resistant to familiar integration strategies. Cloud resources may be built on proprietary rather than open technology "stacks," and their inner workings can't be easily tweaked. What's more, the very fact that cloud services are easy to use and don't require a lot of up-front investment may lure departments and individuals into using them without much thought for how one service relates to other institutional needs. The result could be a cloud version of the segregated information "stovepipes" that CIOs dread.

There is also good news in the cloud integration story. Most cloud services, unlike older business applications, were built for Internet deployment from the ground up, and their "service-oriented" designs can make information exchange easier than it is with traditional applications. Integration middleware products are being updated to extend to cloud services, and a whole class of cloud brokers and integration specialists is emerging to address integration challenges.

It will be increasingly critical to equip staff, students, and faculty with identity mechanisms that give them secure, trusted access to external sources.

Still, it's important to understand that while cloud resources like software-as-a-service may avoid capital expenses and simplify technology management, integration issues—and costs—remain.Ted Dodds, chief information officer and vice president at Cornell University, notes that while the university's Workday project is in early stages, it has already "illustrated one of the benefits of the SaaS model by not becoming sidetracked by issues related toinstitutional data centre and infrastructure needs." But Dodds adds that, as in all large system projects, a great deal of care and effort is required to ensurethe Workday service willwork with Cornell's otherimportant business applications. With software as a service, Dodds says, "the purely technological issues are bypassed, but the integration issues remain."

No enterprise system is an island. Developing integration skills and building tools that facilitate integration will be good ways to prepare for a cloudy tomorrow. Institutions should consider the following:

1. Remember the integration. When considering cloud products like software-as-a-service, integration has to be taken into account both for the costs it will add and for the value it will provide. Some cloud services may stand completely on their own, but others will require extensive interconnections.

2. Focus on identity. As cloud services replace on-premises systems, it will be increasingly critical to equip institutional staff, students, and faculty with identity mechanisms that give them secure, trusted access to external sources. A particularly important area to consider is "federated identity," which allows a user who has identified himself to his home institution to get access to external resources without sending any further identifying information to the outside provider. In Canada, the Canadian Access Federation promotes federated identity in higher education.

Use your buying power to favor cloud services that are open about their operations and standards- based.

Challenge 6: Avoiding Lock-In

One of the advantages of the traditional full-service premises-based IT organization is that it keeps a lot of capability on campus. If a system fails, IT staff can fix it; if a student is having problems with her laptop, tech support can help her. In the many small and large decisions that they make every day, IT administrators can protect the institution from single points of failure and from too-great dependence on vendors and technologies.

The cloud can make an institution more agile by increasing technology choice and reducing the overhead needed to get work done. But it alsoturns a lot of decisions over to third parties, making the institution dependent on vendor choices. Your cloud provider mayrely more on proprietary technologies than your local IT staff would, which in turn may mean that integrating with other campus systems is harder, that data entered into the service is hard to get back out, or that your future choicesare limited in ways difficult to foresee. And if local capabilities atrophy because cloud services have replaced them, switching away from an unsatisfactory provider becomes that much harder. Technology outsourcers have been known to bid low in the early years of a contract, only to raise prices sharply once a customer's internal ability to provide the service dwindles.

Vendor lock-in is not a danger exclusive to cloud services, but it's one to keep in mind as your institution makes its way toward the cloud. To limit the risks, institutions should:

1. Know your provider. Don't treat a cloud service as a black box; be sure you understand how it works, and use your buying power to favour services that are open about their operations and standards-based.

2. Have an exit strategy. Be sure you understand the mechanics of switching away from a service (for example, what data you would get back and what form it would take), and wherever possible, identify alternative providers and/or scope out what it would take to deliver the service internally.

3. Maintain critical skills. While IT physical plants, infrastructure, and staffs are likely to evolve and perhaps shrink as the cloud revolution unfolds, it will continue to be essential to have an independent capability to assess technology, manage it, and integrate its different functions.

Challenge 7: Preparing the Organization

For a long time, we have been accustomed to an "enterprise" IT mentality in post-secondary institutions. We expect that the default source for technology infrastructure, tools, and services is the institution. Things work differently in the cloud. As the cloud atomizes the technology environment and changes large parts of it from a domain of experts into a consumer marketplace, expectations and attitudes will have to evolve as well.

Faculty members and academic unit staff may well celebrate the new choices the cloud brings. Services that might once have required making a business case to the IT organization, waiting for a decision, scrambling to find startup funds, and waiting further while hardware was acquired and software installed, can now be acquired by opening a browser and supplying a credit card number. Leaders who know that bureaucracy and delay have debilitating effects on institutional culture should welcome this rare chance to encourage creativity and self-direction.

The cloud implies a technology organization less dedicated to managing data centres and deploying systems, and more dedicated to user education, integration, and providing safe pathways to external resources.

But liberation from the IT bureaucrats will also introduce new risks. Users will have to be educated to choose wisely, and supervised to ensure they don’t encumber the institution with redundant or unacceptably risky services. Where institutional users aren’t getting adequate support from a cloud provider, they may turn to the institutional IT unit for help, and the IT organization will have to make some difficult choices between leaving users high and dry, or putting resources into supporting services they know little about and do not control.

As the example of user support suggests, things will change for IT staff as well. The cloud implies a technology organization less dedicated to managing data centres and deploying enterprise systems, and more dedicated to user education, integration, providing safe pathways to external resources, and brokering services that might be 0% or 100% cloud-delivered—or anywhere in between. The CIO’s office will evolve accordingly, taking on (in one author’s analysis) new roles like services architect, innovation incubator, business process architect, and information policy manager[9]. IT governance, now used mainly as a tool for allocating scarce IT resources, will evolve into a forum for envisioning and achieving an institutional information strategy.

As cloud services move from the periphery to the core of institutional computing, leaders will have to recognize that the whole community is taking part in, and affected by, an IT revolution. Steps to take to prepare the community include:

1. Educating about cloud services. Institutions will have to get the word out that cloud services present risk as well as opportunity. Users will have to learn to look beyond functional capabilities and consider things like how secure their data will be, how reliable the service is, and whether regulatory concerns are being addressed.

2. Certifying the good ones. Institutions may wish to identify “certified” cloud services that meet basic security, compliance, and performance criteria. The IT organization might offer limited user support for such services as an incentive to choose wisely.

[9] Philip Goldstein (2008). « The Tower, the Cloud, and the IT Leader and Workforce », dans Richard Katz (dir.), The Tower and the Cloud: Higher Education in the Age of Cloud Computing, Boulder (Colorado). [En ligne] dans le site Web à l’adresse http://net.educause.edu/ir/library/pdf/PUB7202x.pdf.

3. Hone the right skills.Just as pedagogical experts advise instructors to be a "guide by the side" rather than a "sage on the stage," IT organizations will have to develop the skills to facilitate and influence, rather than make and implement, technology decisions. Key skills areas to encourage include identity management, network management, security, integration, and policy development.

The greatest risk is to wait for every aspect of the cloud to mature, while somebody else masters its challenges and earns its rewards

Opportunity and Challenge in the Cloud

The cloud does not come with an opt-out checkbox. It is moving relentlessly into consumer markets, driven by its convenience and its complementarity to mobile, information-hungry lifestyles. It will not take long for students who can call a movie out of the sky and watch it on a smartphone, or ask the same device for directions to the nearest gas station, to wonder why their educational institution can't deliver services with the same convenience and simplicity. And cloud services aren't just changing the way we listen to music or organize our photo collections. From learning management systems to textbook publishing and office productivity software, familiar elements of the educational scene are rapidly moving to services-based, cloud-enabled models.Faculty, staff, and students will all be experimenting with these resources, drawing them into institutional life, and comparing them against what the institution provides—as well they should. Institutions need to prepare themselves both to exploit the best results of this experimentation and to mitigate against its most foreseeable dangers.

The risks we outline here are real, and no doubt other ones will emerge as services evolve. But the risks are manageable and outweighed by the opportunities the cloud presents to rationalize IT expenditures, improve educational and administrative services, and make institutions more agile and creative places. Post-secondary education has always combined a remarkable ability to embody deep tradition and self-sufficiency while also embracing innovation and finding new ways to serve its constituents. Responding to the cloud in the same spirit represents perhaps the greatest challenge identified in this paper, and the greatest opportunity as well. The greatest risk imaginable is to wait for every aspect of the cloud to mature, while somebody else masters its challenges and earns its rewards.