

Winter 2010

Educational Procurement JOURNAL

NATIONAL ASSOCIATION OF EDUCATIONAL PROCUREMENT



Cover Story
Standing Up a Campus
Overseas: A Diary, Sort Of

In This Issue
Import Basics

Computing Prediction: Clouds on
the Horizon, with a Chance
of Sunshine on Your Risks



Computing Prediction: Clouds on the Horizon, with a Chance of Sunshine on Your Risks

by **Kerry Kahl, B.A., MBA**
University of Washington

“Cloud computing” has been blowing across the country for several years, taking some organizations by storm while others hunker down to ride out what may only be a short spell of bad weather. Like other innovations, it has its early supporters and adopters—some of whom become uninterested when the “cloud” does not deliver as expected—while many take a wait-and-see approach, or dismiss it altogether.

What is “The Cloud?”

Cloud computing refers to using common IT services such as e-mail, document production, and data storage by means of the Internet, with the underlying hardware and software supported by the service provider. Some organizations have embraced it as a way to provide up-to-date technology services at reduced cost. Others hold off for a variety of reasons, not the least of which is concern about risks in moving to such a new business model. There’s nothing wrong with either approach; it’s a reflection of many variables in an organization, including a “risk appetite” or tolerance, and how many other projects are competing for attention.

Identify Risks before Contracting

Like other technology service contracts, cloud computing needs to have the underlying terms and conditions nailed down to both parties’ satisfaction. A significant aspect is to identify, define, and allocate the risks between the parties. While many of the boilerplate terms and conditions used for other types of technology contracts also apply, cloud computing presents unique risks in that an organization’s data is stored in someone else’s infrastructure, potentially anywhere in the world. What kinds of data you put in the cloud, and what terms the cloud provider will accept can determine the degree to which cloud computing is a good approach for your institution.

The University of Washington (UW) uses an Enterprise Risk Management (ERM) approach to assess cloud computing, as described below. Taking the ERM assessment into contract negotiations, UW has executed agreements with two major cloud computing providers. A set of principles to use in future cloud negotiations has been drawn from that experience, and they are summarized at the end of this article.

Using ERM Tools to Assess Risks

UW developed its ERM program based on the COSO¹ cycle of risk identification—evaluation, response, monitoring—and has applied it on over a dozen types of risks. IT security was an early risk assessment, and UW’s Chief Information Security Officer (CISO) found ERM to be a useful way to communicate risks associated with cyber security and exposure.

When asked to participate on a team looking at how UW might implement cloud computing, the CISO used ERM. Some risk examples include:

Compliance: Failure to meet data management requirements (public records, FERPA); failure to demonstrate “due care” under Federal Rules of Civil Procedure.

Operations: Loss of data integrity, or loss of data access; unnecessary breach notice with associated costs and reputational loss.

Financial: Theft of data resulting in unauthorized expenses (credit card accounts).

UW ERM assessments use standard scales of likelihood (occurrence rare/less than once in 10 years; to almost certain/more than once a year)

Continued on page 14

and impact (estimates of injuries, financial loss, loss of assets, interruption of service, reputation and image).

Ratings of 1 to 5 are plotted on a matrix, with high scores (20-25) being the top, “hot” risks, colored red. The scale of risk ratings is:

- Red (Extreme): Significant capability loss; unlikely to achieve objectives;
- Orange (High): Significantly degrades achievement of objectives/capability;
- Yellow (Substantial): Degrades achievement of objectives/capability;
- Green (Medium): May degrade some achievement of objectives/capability;
- Blue (Low): Little or no impact on achievement of objectives/capability.

Comparing Risk under Different Circumstances

UW’s then current environment held a high interest in making cloud services available to students and faculty, a growing number of whom were already signing up individually for free services. The first draft of the provider’s proposed contract was viewed as being a long way away from addressing the main risk concerns.

The CISO assessed the likelihood and impact of risks under several business alternatives scenarios:

- A. Current environment: Individuals use cloud services, but no institutional policy or contract in place, i.e. keep doing what we’re doing;
- B. Adopt a use policy to inform individuals of appropriate use, but continue without a contract in place;
- C. Negotiate a contract that includes terms to address risk concerns, in addition to an institutional policy.

What the Analysis Revealed

The risk assessment identified different levels of exposure and ranges of alternatives. The current environment, which let individuals do pretty much whatever they want, carried a High risk of failing to demonstrate due care, and a Substantial risk for data thefts.

By adopting a policy that informs users about appropriate use of cloud services, UW would expect to do better, i.e., reduce its exposure to due care and data theft risks (although due care

Is It Right for My Organization?

No matter the type or size of your institution, a risk assessment can provide a structured review. The answer will be unique to your organization, “Are these risks we can accept, or do we need to manage or mitigate them to a level we can accept?”

When Might I Do a Risk Assessment?

Even though a service contract may be new for your organization, is it fairly well established in the marketplace? If yes, a risk assessment may not add value to your planning.

If, however, it is a new offering, an assessment can help identify risks that will be important to address in your contract. For example, ensure that your organization continues to own all of its data stored on the vendor’s systems.

was still assessed at the Substantial level). Exposure to loss of data integrity and access would be reduced.

Moving to the third business alternative, negotiating an agreement addressing these concerns and obtaining satisfactory terms would lead to improvement on almost all identified risks except for unnecessary breach notice which was raised to the Red (Extreme) risk level. Cloud

providers made contractual assurances for data protection and security; what they had not agreed to was access to their files when a breach may have occurred. UW needed to do its own forensics on what information may have been accessed. Without that ability, it is more likely UW would broadcast breach notices, even in cases where it would not be necessary (such as if the actual limits on unauthorized access could be demonstrated).

Lessons Learned

UW is confident that the contract terms—with Google for Apps for Education, and with Microsoft for Live@edu—address risks in a way that cloud services can be offered to most faculty and staff and students. Other institutions, some even several years ago, have moved their student e-mail to the cloud, but UW is among the first to offer it more broadly to the campus community. There are exceptions: individuals who handle data restricted for export purposes are not to use the cloud; and there is a ban on using the cloud for any patient/HIPAA related data.

What the risk assessment does not evaluate is the opportunity and benefit that comes from cloud services—the ease of collaborating on instructional and research projects, and access to evolving tools for the classroom and office. When making a decision to pursue cloud computing, weighing such benefits is as important as assessing the risks.

By adopting a policy
that informs users about
appropriate use of cloud
services, UW would expect
to do better, i.e., reduce its
exposure to due care and
data theft risks (although
due care was still assessed
at the Substantial level).

Key Principles for Cloud Contracts

Most of the following terms have their counterparts in good contract language. Each institution has its own version and preferred wording on these clauses to use as a starting point. The key principles identified by UW include:

- **Security:** Meet industry standards; conduct security audits; vendor responsible for security breaches;
- **Indemnification:** Mutual indemnity for negligent acts and omissions preferred; do not indemnify for behavior of end users;
- **Limitation of Liability:** Prefer no limit on vendor's liability except to extent loss is caused by University;
- **FERPA:** Vendor is a school official and must accept certain duties;
- **Data Ownership:** University maintains ownership of data stored on vendor's systems.

One more bit of advice: Don't fly into the cloud without an exit strategy. Know how the contract terms allow retrieval of data deposited in the cloud. It is unclear what the sustainable business models will be for the long run among the various cloud providers, and as the clouds become more populated with valuable data, they are likely to become more attractive targets for hackers.

Risk Assessment = Contract Terms: A Few Final Words

Whether it is cloud computing or the next, new must-have technology that is enticing your institution, applying a risk assessment model is a good starting point. It provides a set of top risks to address in the contract. Everyone then understands what may be at risk, even if the organization goes forward to take advantage of the benefits that the technology is expected to deliver.

Remember, behind every cloud, the sun is still shining.

¹COSO is the Committee of Sponsoring Organizations of the Treadway Commission. The Treadway Commission, a private-sector initiative, was formed in 1985 to inspect, analyze, and make recommendations on fraudulent corporate financial reporting.



Kerry Kahl, B.A., MBA, is a long-time Member of NAEP, having worked in the University of Washington (UW) purchasing office for more than 25 years. He served as NAEP Northwest Regional President and on the E&I Cooperative's Board of Directors. Kerry currently splits his time between Enterprise Risk Management, helping assess and prioritize a wide range of risks at the university, and in UW Information Technology, planning and overseeing major IT projects and acquisitions. E-mail: kkahl@u.washington.edu.



Planning on exhibiting at our 90th Annual Meeting in Memphis? Interested in partnering with us as one of our valued Sponsors?

Call Toni Valenti or Jackie Harget at 443.543.5540 for more information today!

meet the new department chair.

Say hello to node,[™] a mobile and flexible chair designed for quick, easy transitions between classroom configurations. The node chair supports an active learning environment while keeping the student more comfortable, more connected, and more engaged. Learn more at steelcase.com/node.



Steelcase
Education Solutions

The node chair is available via E&I's **competitively awarded** Steelcase contract. Contact your Member Services Rep today or call 734-326-3920 for more information.



Lower Costs for Higher Ed