Much recent discussion has focused on the pros and cons of cloud computing. While institutions may be attracted to benefits such as rapid deployment, flexible scalability, and low initial start-up cost, they are right to be simultaneously concerned about risks of computing in the cloud, including those related to data location, level of service, and security infrastructure. For institutions that have determined that the benefits of cloud computing outweigh the risks, this session provides suggestions to help mitigate those risks by focusing on cloud computing contracts and related issues. There are no simple right or wrong answers that apply across the board; each contract clause must be evaluated in the context of an institution’s needs and tolerance for risk.

While IT managers are likely more familiar with managing technology, when it comes to the cloud, they need to shift their perspective to managing contracts. Unlike IT purchases in which a university buys a product and walks away, cloud agreements often entail developing and managing a complex long-term relationship with a vendor. In such relationships it is critical that the vendor understand the client’s expectations and that the client has a means for ensuring that the vendor meets agreed-on requirements. Such considerations require different skill sets on the part of the university, first in defining the scope and terms of an agreement through contract negotiation and then in actively managing the relationship with the vendor during the lifetime of the agreement. Clients should negotiate key elements of the contract, and such negotiations generally cover four broad areas:

- Service-level agreements
- Data processing and storage
- Infrastructure and security
- Vendor relationship

**Service-Level Agreements**

While there are many dimensions of cloud computing, for our purposes here we will use a definition from Gartner that describes cloud computing as “a style of computing in which scalable and elastic IT-enabled capabilities are provided as a service to consumers using Internet technologies.” A key word in this definition is “service.” Because many dimensions of a cloud computing agreement are governed by the contract, the contract must specifically spell out expected service level agreements (SLAs). In that regard, the contract needs to be clear about expectations for uptime and downtime, response time when things go awry, latency, infrastructure, and security.

For example, contracts regularly reflect the expectation of 99.9 percent uptime. While that sounds good on the surface, part of due diligence means asking whether that amount of uptime meets an institution’s specific needs. Contract negotiators need to understand the...
specific parameters of downtime. For example, will planned downtime be scheduled at times that best suit the business needs of the university? Do agreed-on parameters for downtime cover circumstances beyond the control of either the client or the vendor? What about downtime due to scheduled maintenance? Such questions underscore the importance of taking pains to carefully and fully define terms in SLAs.

Once SLAs are in place, they need to be enforceable via pre-agreed remedies. Contracts should include provisions for what a vendor will do to correct errors and penalties that provide a financial credit if things do go wrong. As a benchmark, Gartner advises that penalties be negotiated at between 10%–20% of the total value of the contract. Anything less may not get the vendor’s attention; anything more might be a deal breaker.

It is important to codify how and when a financial penalty would be assessed and credited. Remember, though, that the goal of such remedies is not to earn credits but to motivate the vendor to provide high levels of service. There should be no limit, however, on the cumulative value of penalties.

In order to enforce the SLAs, a client must have a means to track performance. This typically includes the ability for a client to audit vendor performance records and access daily quality statistics.

Data Processing and Storage

Given that institutional data will reside in the cloud, it is important to affirm continued institutional ownership of those data. This question has been evolving since the advent of cloud computing, but more vendors are starting to acknowledge institutional ownership of data, even in boilerplate contract language. In addition, depending on how institutional data are processed, it might also be necessary to negotiate ownership of any results of data processing.

It is also important to negotiate the disposition of data should the university decide to contract with a different vendor in the future. The contract should delineate the client’s rights to access and retrieve data after a contract has ended and the process by which that will be done, including a time frame and a format for the data. In this context, the contract should also describe emergency provisions should it become necessary for the university to access data under unexpected circumstances. The contract should also define the vendor’s obligation to destroy data after the contract ends.

The contract should also spell out what happens in the event of a data breach, being specific about the vendor’s obligations should this occur. Key considerations include requirements for when and how the vendor would notify the university about a breach, what details the vendor will be expected to provide, and what corrective action the vendor will take. In the case of a data breach, the service provider should be contractually obligated to indemnify the institution.

Knowing the type of data that the institution will be storing with the vendor will help clarify what factors concerning data security should be delineated in the contract. HIPAA or FERPA data, for example, have higher thresholds for security than non-sensitive data.

One of the benefits—and risks—of having data in the cloud is that those data can be processed in locations around the world. That can be helpful for maintaining data backups and sustaining business continuity, but it also comes with a certain degree of risk that contracts need to address. One specific issue to clarify, for example, is what jurisdiction’s laws apply to the data.

The contract should also address the vendor’s obligations should data placed with the vendor be subject to legal action, such as a subpoena. The contract should be specific, for example, about the time frame in which a vendor needs to notify the client about such requests for data, ideally before the vendor moves to meet that request.
Infrastructure and Security

The virtual nature of cloud computing makes it easy to forget that the service ultimately depends on some type of physical infrastructure. The contract needs to specify infrastructure and security requirements and practices, covering such considerations as business continuity, firewalls, encryption, and physical security.

To verify that the infrastructure is indeed protected, a right-to-audit clause should be part of the contract. This should clarify the client’s rights regarding third-party audits, certifications, and any resulting reports. There are no formally recognized standards for certification of cloud computing, but several types of audits have become standard practice in the industry:

- **SAS 70, Type II.** Technically an auditing and reporting process rather than a certification process, the SAS 70, Type II reporting format was issued by the American Institute of Certified Public Accountants (AICPA). The AICPA is expected to replace this format in June 2011 with a new format called the Service Organization Controls report, or SOC 2.
- **FISMA.** The Federal Information Security Management Act (FISMA) provides relevant standards and guidelines.
- **ISO 27001.** Issued by the International Standards Organization, ISO 27001 provides specific guidelines for a management system that controls information security.

While these types of audits provide a certain degree of security assessment, universities need also to write into the contract their right to conduct onsite inspections of a vendor’s infrastructure and security practices, ideally at least once a year. If an institution does not have the resources for site visits, an alternative approach would be to append the vendor’s specifications for security and infrastructure to the contract as a minimum requirement. Vendors might push back on the costs of security audits, a concern that might be mitigated by capping such costs in the contract.

The contract also needs to address the possibility of loss of service due to unforeseen circumstances and should include specific plans for disaster recovery and business continuity. The contract should also address what would happen if any of an institution’s data are lost or damage under such circumstances.

Vendor Relationship

Because a client’s negotiating power is strongest prior to signing the contract, it is vital to codify in advance not only the conditions under which an institution would continue to use the vendor’s services but also the conditions under which such services might be changed or terminated. Changing services can be the costliest aspect of cloud computing. Universities, therefore, need to plan for changes or expansions that might be necessary during the lifetime of the contract, as well as for what will happen concerning the termination of the contract and post-termination. It is good to anticipate, for example, pricing caps for renewing the contract, and these caps can be tied to a specific consumer price index, for example, or based on a percentage increase.

The fluid nature of the cloud means that functionality can be deleted as well as added over time. Contracts should be explicit, therefore, about what products are being contracted for and what functionality the client is purchasing. Because scalability is one of the benefits of cloud computing, the contract should protect the client’s ability to use only the level of service that is needed. Expansion of service should be at the client’s option, and clients should protect themselves contractually and financially should they decide to reduce services.

In terms of negotiating terms for the end of the agreement, the contract should offer the client the right to terminate the agreement at will, without cause or penalty. At the same
time, it is important to define relatively narrowly the vendor’s rights to discontinue. One consideration is how much time a university would need to replace a contracted service should the vendor discontinue that service. If possible, link a vendor’s ability to terminate to a specific event or conditions, with provisos about when the vendor has to notify about any decision to terminate and giving recourse in terms of appealing the decision before it is finalized.

Cloud computing is an evolving field, and another factor to consider is whether the vendor is subject to merger or acquisition by another provider. Part of due diligence, therefore, is to research a vendor’s stability, leadership, long-term viability, and finances. Contracts should be written such that their terms are binding on any successors to a vendor and that they assign successor companies with the same responsibilities that have been negotiated with the principal vendor.

Outsourcing of services by vendors is also not uncommon. Contracts need to protect the client should outsourcing occur and ensure that the vendor continues to have responsibility to the client for all contractual obligations even when services are completed by a third party. Contracts should require vendors to notify the client any time a third party is involved.

To be successful, contract negotiations need to include a wide range of people, units, and functions across campus. Institutions that engage in such negotiations should regularly document effective practices to inform and improve future negotiations.