This paper is the second in a series on Preparing the IT Organization for the Cloud from the ECAR-CLOUD Working Group. For institutions that have decided to adopt cloud services, transitioning to the cloud presents both opportunities and challenges. This series provides guidance to help institutions effectively prepare to address these challenges. More information can be found at the ECAR working groups website.

Introduction

Educational institutions increasingly include cloud services in enterprise IT portfolios as well as enable bring-your-own-everything cloud tools. IT governance—traditionally a formal process to connect IT investments to business outcomes—is in danger of becoming outmoded unless it evolves to include cloud services. Cloud solutions have changed the way that IT decisions and investments are made, primarily because cloud solutions can be adopted easily by departments and individuals for a very low initial investment, outside the institutional decision-making process. By implementing cloud-aware IT governance, the institution can better coordinate cloud offerings and reduce the risk of duplication, missed buying-power opportunities, resource inefficiencies, and lack of a clear service definition to the community.

In addition, cloud-computing investments can represent a change from capital spending (which historically has been used for expenses such as equipment) to operational spending (which has typically been used for subscriptions and maintenance contracts). IT governance that considers cloud computing will help aid in the analysis of the overall investment, including more fully understanding the qualitative and quantitative factors that are analyzed in a complete total cost of ownership (TCO) calculation.

Cloud computing also represents a shift from a campus-focused view of privacy and security to a model that relies on trust-based partnerships with global firms. Cloud computing invites a transition from IT-centric projects to projects that drive toward business goals. All of these aspects of cloud computing have implications for IT governance.

A cloud-aware IT governance strategy helps increase awareness of cloud computing throughout the organization and will help highlight the importance and considerations that come with adopting cloud solutions. By becoming cloud aware, IT governance can work to bring appropriate campus constituencies together to inform strategic IT decisions that embrace the realities of cloud use on campuses, balance cloud risks with opportunities, and support both top-down executive goals and bottom-up user needs.
What Is Cloud-Aware IT Governance?

A mature IT governance model articulates the institutional IT decision-making process. Definitions of IT governance are many, but they often approach the issue from a top-down perspective, with assumptions that organizations are making IT decisions through a single, unified voice and body. Cloud-aware governance ensures that all stakeholders understand the appropriate uses of cloud computing and that IT projects and initiatives support the institution's cloud-computing strategy. With cloud computing, the decision to use cloud services for the business of education now rests with many more individuals. Faculty can use cloud-based educational tools to support student engagement, students can use free file storage and collaboration services to work on projects, and staff can purchase software-as-a-service business applications to wholly replace legacy campus systems, all without involving IT or any institutional governance process.

In this new reality of an increasingly bottom-up nature of IT decision making due to cloud services, higher education organizations must find a new way to develop and operate IT governance. Therefore, a good IT governance model that incorporates cloud should include the following key functions:

- Provide a mechanism to allow for both top-down and bottom-up needs to be included in the process
- Provide decision-making rights and accountability frameworks that are agile and easy to use by IT decision makers
- Protect the institution and its interests
- Identify and manage risk
- Address privacy and security issues, including policy and regulatory compliance
- Ensure that both administrative and academic units are participating fully in the process, representing business, IT, legal, risk, procurement, compliance, and all other institutional perspectives
- Ensure that both central IT and decentralized IT units are coordinating needs and opportunities

Cloud-aware IT governance programs take these factors into consideration and integrate them into the institution’s existing IT governance processes. Ensuring that IT governance is optimized for agile decision making, that the needs of the users are visible and accounted for, and that all stakeholders are at the table will encourage the organization’s users to utilize the IT governance process.

Why Cloud-Aware Governance?

Whereas IT governance models have been widely studied and strong guidance exists for them, cloud-aware IT governance models are still in early stages of maturity, just like cloud computing itself. However, certain attributes of cloud computing in higher education magnify the importance of the factors discussed above:

- Cloud services require agility from both IT and the broader governance process—because users can easily use free cloud services or acquire them with purchase cards, there is often little patience for waiting until the institution provides a similar service or approves the use of such a service.
- Distributed IT units with smaller user bases are often under pressure to think locally and act quickly on behalf of their users, which can lead to diversity and duplication of services. On the other hand, central IT units can often learn from, and apply knowledge from, the distributed IT unit experience with cloud services. This knowledge sharing is vital in cloud adoption and governance.
Collaboration between distributed and central IT units as it pertains to the use of cloud services is important to ensure that both groups are aligned with institutional goals, direction, and risks.

Due to the ease of adoption for cloud services, usage by the broader community is now informing the needs and trends for the institutional strategy.

Security, accessibility, financial, and legal concerns may be more layered and complex in cloud computing scenarios. For example, a single solution could include many cloud vendors, requiring multiple contracts, risk assessments, and support considerations.

Cloud computing creates a dynamic to which most of higher education IT has not been accustomed. Business units are now able to easily procure cloud services independent of the IT unit and without needing IT expertise in the business unit. This allows the higher education community to acquire desired services quickly and easily and can lead to business productivity far faster than older IT approaches. The adoption of a cloud service entails a wide range of implications, from complying with policy and external regulations to protecting intellectual property and integrating security and risk-mitigation controls. A cloud-aware governance process should assist the community with managing these considerations by providing a framework to easily acquire and use services in a fast and efficient manner that addresses institutional risks and compliance while supporting bottom-up IT decision making in the business units. In addition, by adopting an IT governance strategy that accounts for cloud computing, institutions can consider and accept risks for the use of the services campus-wide, rather than relying on individual users and/or departments to accept that risk.

**Incorporating Cloud into IT Governance**

Institutions will approach cloud IT governance in different ways. In every institution, there will be a continuum of IT decision making, ranging from the individual who subscribes to a $50-per-year cloud service to the formal institutional adoption of an enterprise cloud service. Many institutions already have functioning IT governance processes in place, whereas others may want to use the impact of cloud computing to begin or overhaul current IT governance processes. Each institution will need to establish a cloud-aware IT governance process that is agile and sufficiently light-handed to be appropriately applied to decisions at all points of the continuum. Whether governance is formally defined or less mature, several key elements are factors for incorporating cloud into an institution’s IT governance process.

**Engage Stakeholders**

The effective adoption of cloud computing services should involve key stakeholders from various units across campus including, but not limited to, business process owners, IT, procurement, vendor management, accessibility, legal, security, policy, privacy, and risk management. These key stakeholders often drive the adoption of cloud solutions because they address business needs. The inclusion of stakeholders from across campus helps integrate the institution’s culture and goals into an IT governance model that has a clear decision-making process, prioritization methodology and practice, and resource oversight.

Many campuses organize IT governance to include a diverse set of stakeholders of faculty, staff, and students from both centralized administrative departments and decentralized academic units to work together in the institution’s best interests. Cloud computing’s growing ubiquity and low barrier to entry is leading to a growing impact on a broad set of university functions. As a result, administrative and academic units are foundational to IT governance participation. In the past, business and academic units
may have engaged an IT governance process due to funding approval requirements, and others may not have engaged the IT governance process at all. Therefore, helping these stakeholders understand the value of governance is an opportunity to educate them on the potential for cost saving, expense sharing, risk mitigation, and resource collaboration. As IT units, we gain the expertise of these stakeholders as it pertains to the institutional culture and knowledge that are vital in cloud service design and delivery.

Another key consideration in IT governance as it relates to cloud services is faculty engagement. Many cloud services are designed to meet classroom and research needs, and a significant amount of risk may come from storing sensitive student and research data in the cloud. Broadly representative faculty participation in cloud governance will help identify these issues and communicate the consequences and best practices. The student voice should also be represented in IT governance, and cloud governance is no exception. Particularly in the teaching and learning technologies and research computing domains, students provide valuable insight into the suitability of considered services. Making the effort to study what cloud services faculty and students are using as part of the teaching and learning process may help inform cloud strategy.

Rightsize Your Governance

The ease of acquisition of cloud computing makes it challenging to manage top-down decision making around the adoption of cloud services because anyone can make the decision to purchase or sign up for a cloud service. An established and effective IT governance structure that is integrated into the campus culture will provide the campus community with an understanding of how decisions are made and who makes them. Once the right stakeholders are engaged, the IT governance group can work to decide on the best approach to achieving the core goals of cloud-aware IT governance—which might include reducing cost from duplication, protecting sensitive and confidential data, and providing better service to the community—and bring transparency and accountability to cloud decision making. This process may include some purposeful relinquishing of central decision making by an IT governance group in favor of a shared and more decentralized approach. In other words, cloud decisions can come top down and bottom up, but the key is that they are made in a coordinated, fully transparent way.

If cloud-aware IT governance is to be agile, all decisions cannot be made by governance bodies. Just getting all the parties to a meeting might prove to be a tremendous challenge, let alone asking them to address all IT decisions. However, clarity is critical regarding whether a decision may be made locally or must be addressed by IT governance—and, if so, with clear reasons as to why it is included in governance (e.g., in the case of sensitive data). Both the campus community and those involved in IT governance will benefit from this clarity if they are engaged in an open, transparent process that views the institution’s technology needs in a holistic manner (rather than an antagonistic one).

Good IT governance addresses issues of prioritization and, to some extent, portfolio management. With cloud services, the portfolio of IT services used by the university may grow rapidly. Cloud-aware IT governance has a role in coordinating the use of these services by communicating their availability and prioritizing needs to avoid duplication of effort and to leverage economies of scale. Often this coordination requires that governance processes move quickly to collaborate with individuals or academic/business units as needs arise to lessen the risk that those individuals/units might proceed without the benefit of the governance process.
Good cloud-aware IT governance does not happen by accident. An effective structure must be deliberately designed—although it may take some trial and error—accounting for the university's culture and strategic goals. Institutions with the most effective IT governance processes explicitly dedicate staff resources to facilitating the governance process. A cloud-aware process requires regular review and adjustment to ensure continuous improvement.

Ask the Right Questions

In general, it would be wise to create a set of questions that your institution could ask of every individual or department voicing a need for cloud services. These questions should help the requestor gauge the sensitivity of the data, the degree to which the system will be business critical, and the requirements for uptime (recovery time objective) and data loss (recovery point objective). A similar questionnaire could be used to evaluate cloud providers, as well. Questions of the cloud vendor might vary, depending on your institutional context, and could cover considerations such as data integrity, data sensitivity, data location, encryption, disaster recovery, business continuity, the availability of the service, service elasticity, the location from where the service emanates, and cost (including exit costs). The goal is not to be encyclopedic but to ask pertinent questions to evaluate risk versus business needs and to provide requestors with this information to help evaluate cloud services.

If sufficiently clear, well constructed, and simple to use, these questions can be disseminated throughout the institution so that business, IT, and individual decision makers are aware of risks and benefits and can take them into account.

Your institution should consider establishing criteria for or constraints on IT decision making that reflect the institution’s attitude about cloud computing. For example, if your strategy will be “cloud friendly,” then questions such as the following might be considered:

- Have you examined cloud options for this service as well as on-premises options?
- If you have rejected cloud options, what were the reasons for doing so?
- Have you applied the same criteria for security, compliance, data control, etc., to both the cloud services and the on-premises options?
- What are the medium- to long-term staffing and infrastructure implications of your decision?

If your institutional attitude about cloud services is more cautious, then different questions might be in order, such as these:

- If you are considering a cloud solution, have you established adequate controls to ensure that sensitive and confidential data are protected?
- Have you asked whether an existing on-premises solution can meet your needs?

Your IT governance team should be drawn from many areas of the institution. Working together, such a team can collectively achieve a holistic perspective through which to view and establish an enterprise-wide cloud strategy, identify and establish an organization’s risk-tolerance thresholds, and establish guidance and best practices regarding the effective evaluation and adoption of cloud services. This team can be a single source of expertise to evaluate proposed solutions. If the governance body is establishing an enterprise-wide strategy, its composition is particularly important—it should include people who are authorized to speak for the organization. The level of personnel involved may vary if the goal is to make a
recommendation rather than establish a strategy. To ensure engagement with the requestors of cloud services, the governance body may ask key individuals from business units, faculty, or others to participate jointly in reviews. This can help ensure buy-in and engagement so that the governance process does not feel like a “black box” to the institution but rather a transparent, engaging process.

Establish a Cloud Review Process

A review of cloud services prior to adoption is best incorporated into existing IT governance processes. Develop a consistent process that builds confidence through responsiveness. Governance should empower the institutional community, not create frustration.

To help build in both consistency and speed, you should establish criteria for your institution to consider when adopting a new cloud service or making a significant change to an existing cloud service. For example, some institutions may exempt IT decisions supporting research activity from review, or certain tools may be preapproved for community use. These criteria will be in addition to existing criteria normally considered during an IT governance review in an effort to consider additional cloud-specific concerns. These may include (in no particular order):

- **Existing services.** Before adopting a cloud service, the institution should assess whether any existing services already provide the desired features or if such services can be modified to do so adequately and cost-effectively. A campus service catalog can help with this assessment. The review may also trigger an assessment of whether it would be beneficial to replace existing services with the cloud solution.

- **Accessibility.** The lack of customizability of many public cloud services means that accessibility cannot be an afterthought because the cloud provider may not be prepared to remedy deficiencies.

- **Data sensitivity.** If sensitive data are involved, a review should be triggered to assess the risks and benefits of storing them in the cloud. These may include research data subject to export controls, personal health information (PHI) under HIPAA, student records protected by FERPA, or sensitive university data such as personnel records.

- **Security and compliance.** Depending on the nature of the data stored in the cloud, varying levels of security and compliance review may be required. Organizations may wish to establish a baseline or checklist that would apply to all cloud services, with criteria for additional review.

- **Exit strategy.** Before making substantial investments in a cloud service, an institution should insist that an appropriate exit strategy has been considered and defined. For example, if petabytes of data are stored with a cloud provider, there are practical limitations for retrieving and storing that data should it be desirable to terminate the contract or change providers or if the provider stops providing the service.

- **Changes to campus business practices.** The implementation of a cloud service may impact the way the university processes, stores, or transmits data. Further, the rapid and frequent changes associated with many cloud services may require additional flexibility in university business practices. The impact should be well understood prior to investing in the service.

- **Staff effort.** The adoption of a cloud service may require skilled effort to integrate the service with existing campus infrastructure or applications, and it may even increase the need for end-user support. A review should include an assessment of staff effort required. It is desirable to establish a threshold for additional staff effort that would trigger a review—e.g., an FTE’s worth of effort, either as an incremental position or for the repurposing of an equivalent amount of staff time.

- **Costs.** A review should identify all costs. Cloud services sometimes bring charges that are not traditionally accounted for in an on-premises system, such as storage-transaction or data-transfer
charges. Additionally, the elastic nature of cloud computing means that dynamic usage spikes could result in unexpected charges. A review should ensure that adequate controls are in place to manage costs. A threshold should be established that will trigger review. However, cost should not be the only factor that can trigger a review.

The IT governance team needs a communicative, transparent, and timely approach. The requestor should be kept informed of the status of a given cloud service review.

**Conclusion: A Community Approach to Cloud-Aware IT Governance**

Successful IT governance efforts clearly communicate the importance of effective governance to the campus community and engage both central and decentralized units for top-down and bottom-up decision making. The ease of deploying cloud solutions without the involvement of central IT makes this engagement particularly important. Individuals and business units considering cloud offerings may not understand complexities around important issues, such as:

- Integration with identity and access management systems
- Integration with enterprise data sources
- Support requirements
- Security requirements and compliance obligations

Incorporating cloud into the institution’s existing IT governance process helps develop a culture that keeps the best interests of the institutional community at heart.

IT governance is about IT decision making, and good IT decisions should be well understood and widely accepted. Building the right IT governance team will go a long way toward achieving those two objectives. With the increasing availability of cloud solutions, it has become clear that IT decisions are appropriately made in many parts of an organization—what is important is that all IT decisions address the right institutional questions. A strong IT governance team can help achieve that goal.

**Additional Resources**

- Preparing the IT Organization for the Cloud, ECAR working group series.

- University of Wisconsin–Milwaukee Cloud Services Advisory Board Presentation, slides and a checklist for review and approval of a “Cloud Enabled Software, Processing or Data Services/Storage Contract,” February 19, 2013.


Authors

Special thanks go to the following ECAR-CLOUD Working Group authors of this report.

**Sol Bermann**
Privacy Officer
University of Michigan–Ann Arbor

**Debbie Carraway**
Assistant Director, Infrastructure, Systems, and Operations
NC State University

**Michael Cato**
Chief Information Officer
Vassar College

**Mike Chapple (Co-Chair)**
Senior Director, IT Service Delivery
University of Notre Dame

**Alan Crosswell**
Associate Vice President and Chief Technologist
Columbia University

**Thomas Dugas (Co-Chair)**
Associate Director for Client Operations
Carnegie Mellon University

**Bob Flynn**
Manager, Cloud Technology Support
Indiana University Bloomington

**Chad Haffenden**
Consultant
University of Washington

**Sharon P. Pitt**
Deputy CIO
George Mason University

**Kim Round**
Director of Instructional Technology
Saint Anselm College

**Miguel Soldi**
Assistant Chief Information Security Officer
University of Texas System

**Oren Sreebny**
Senior Director, Emerging Technologies and Communications
University of Chicago

**Steven A. Terry**
Director of Enterprise Applications
Denison University

**Thomas Trapper**
Senior IT Commodity Manager
University of California, Office of the President

**Joseph Vaughan**
CIO and Vice President for Computing and Information Services
Harvey Mudd College

**Bruce Vincent**
IT Architect and Technology Strategist
Stanford University

**Bill Wrobleski**
Director, Technology Infrastructure
University of Hawaii

**Gabriel Youtsey**
Chief Information Officer, Division of Agriculture and Natural Resources
University of California, Office of the President
Notes

1. This change is part of the impetus for a new ECAR working group that is focusing on IT Funding Models: Current Limitations and Needs.

2. The recently published ECAR working group report TCO for Cloud Services: A Framework provides a tool for calculating the total cost of ownership. Application of the TCO framework will “help institutions effectively understand and analyze all costs associated with running a system or service on-premises versus moving it to the cloud, and more accurately identify the cost to a specific department as well as the cost to the institution as a whole.”

3. For instance, Weill and Ross define IT governance as “the decision rights and accountability framework to encourage desirable behavior in the use of IT”; see Peter Weill and Jeanne W. Ross, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results (Cambridge, MA: Harvard Business School Press, 2004): 8. Gartner’s definition is more specific about what the desirable behavior should be: “Governance is the decision framework and process by which enterprises make investment decisions and drive business value”; see Heather Colella, “Governance Best Practices for Midmarket IT Leaders,” Gartner, May 16, 2014.

4. For example, Harvey Mudd College has developed a set of questions that they ask of SaaS and other cloud service providers.

5. It should be noted here that there are cloud integration tools now aimed at what Gartner calls the “citizen integrator”; these promise to greatly simplify integration efforts. Examples include Dell Boomi and Snaplogic.