



# MANAGING THE RISKS OF OPERATING IN THE CLOUD

BY PHILIP D. PORTER AND MICHAEL E. LARNER



## Foreword

Cloud computing is a complex, rapidly evolving phenomenon with long-term implications for IT infrastructure and the delivery of many campus services. The National Association of College and University Business Officers (NACUBO) with assistance from EDUCAUSE and some leading business partners is currently undertaking an educational initiative to prepare business officers for these upcoming changes. The initiative includes member research regarding current practices and a series of white papers, webcasts and live programs.

The following white paper reviewing the risks for cloud computing is the second of several that are being written as part of this initiative. A previous paper described the business case for cloud computing and future papers will address some of the issues involved in an audit of a cloud provider. The combination of initiatives will provide business officers with a solid foundation in cloud computing and prepare them for more productive conversations with chief information officers and cloud providers.

Thanks to Michael E. Lerner and Philip D. Porter, of Hogan Lovells for authoring this white paper, SunGard Higher Education for preparing the previous paper and Microsoft for their continued support of this discussion and the many other individuals who have donated their time and expertise to this project. We welcome feedback regarding our efforts and suggestions for future refinements in what promises to be an interesting and ongoing conversation for many years to come.

Roger V. Bruszewski  
Vice President for Finance and Administration  
Millersville University  
Chair, NACUBO Shared Assets & Services Ad Hoc Committee  
[roger.bruszewski@millersville.edu](mailto:roger.bruszewski@millersville.edu)

# MANAGING THE RISKS OF OPERATING IN THE CLOUD

For years, your institution has probably been “operating in the cloud”—using one or more technology assets (hardware, software, or networking capability) remotely, via Internet browsers, instead of installing them on campus. You might, for example, rely on a third-party vendor, rather than the institution’s IT team, to operate and manage website development and hosting or to provide software for delivering distance education courses.

Moving such operations to the cloud may have created little risk. As the types of cloud offerings have multiplied, however, so have the risks. In fact, Gartner, an information technology research and advisory company, predicts that the worldwide market for cloud services will total \$148.8 billion in 2014. That represents an increase of more than 250 percent over the worldwide market in 2009<sup>1</sup>. Given marketplace interest of this magnitude, companies ranging from large, well-established companies with strong track records—such as Amazon.com, Google, and Microsoft—to recent start-ups, often with little experience and thin capitalization, now offer cloud-based services.

Because operating in the cloud does not require the purchase of products other than workstations, cloud offerings are referred to as services. Productivity software applications—the technology assets most commonly offered through the cloud—are called Software as a Service (SaaS). Data storage, data security, and networking capability are examples of Infrastructure as a Service (IaaS). Although less common, Platform as a Service (PaaS) is generally understood to mean technology assets useful for development of software applications.

## EVALUATING A VENDOR

Before moving more of your institution’s operations to the ever-expanding cloud, you and your CIO should carefully check the prospective vendor’s credentials to verify, insofar as possible, that the vendor is capable of providing reliable services. The rigor of this inquiry will depend on three factors:

### 1. The nature of the proposed services:

- Are the services mission critical to your institution’s operations or of tangential importance?

- If a serious failure of the services occurred, where would the consequences fall on a spectrum of catastrophic to merely inconvenient?
- Will the services require modification to fit the institution’s business processes? If so, is the vendor willing to modify the services?

### 2. The nature of data being transferred to the cloud:

- Must the data must be accessed and/or processed on time-sensitive schedules?
- Does your institution consider the data confidential?
- Do federal and/or state laws and regulations obligate your institution to protect the data?

### 3. The nature of the vendor’s proposed contract:

- How close does the contract come to meeting your institution’s needs?
- If the vendor is not well-established or strongly capitalized, what protections does the contract offer against the risk of vendor failure?

Given the competitive market for cloud computing services, not all vendors will capture the market share or achieve the operating efficiencies required for survival. Even a large, well-established company may be experimenting with a cloud offering rather than making a long-term commitment. To ensure you choose a vendor that will endure, check its financial stability; even if you rely on a Dun & Bradstreet report, also consider reviewing the vendor’s financial statements. In addition to checking customer references—ideally, other higher education institutions—look for comments about the vendor in blogs and other social networking media.

Ask your CIO to review the prospective vendor’s disaster recovery/business continuity plan to assess preparedness to continue providing the cloud-based service should a catastrophic event occur. Such plans customarily offer recovery time objectives or targets rather than guarantees. Nevertheless, compare the vendor’s readiness to address service interruptions with your institution’s ability to restore operation of the installed technology assets that the cloud services are intended to replace.

Vendors of cloud services often quote prices that are lower than those for comparable installed assets by crafting a one-size-fits-all service offering. While the price may be attractive, the service offering may not perfectly fit your institution’s business needs. If that’s the case,

<sup>1</sup> Rachel King, Flextronics, Siemens Lead ‘Big Shift’ to Cloud Computing, BLOOMBERG BUSINESSWEEK, Dec. 6, 2010 ([http://www.businessweek.com/technology/content/dec2010/tc2010126\\_395358.htm](http://www.businessweek.com/technology/content/dec2010/tc2010126_395358.htm))

# MANAGING THE RISKS OF OPERATING IN THE CLOUD

determine whether the vendor is willing to adapt the services to the institution's needs—and how much such adaptations would cost. Also ascertain how much your institution would spend to modify its business processes to accommodate aspects of the cloud services that cannot be changed (or for which changes would be too costly). Factor in whether your institution's stakeholders would resist changes to business process changes and therefore undermine adoption and use of the cloud services.

Ideally, before any negotiations begin, meet with both your CIO and general counsel to evaluate a prospective vendor's service agreement. One-size-fits-all service agreements, like one-size-fits-all service offerings, enable cloud services vendors to offer lower prices. Large, well-established vendors may be unwilling to change their services agreement (except for very high-revenue transactions). In anticipation of that possibility, determine the extent to which the service agreement addresses the risks of cloud computing and whether your institution can accept the way the vendor mitigates those risks. Be particularly wary of any service agreement that gives the vendor the unilateral right to change material terms and policies related to the cloud services.

## SERVICE LEVEL COMPONENTS

When a technology asset installed at your institution ceases operating or operates improperly, the IT team has primary control over the response, which may include application of a software patch, installation of a hardware spare part, or acquisition of replacement or additional technology. When the same technology asset is hosted remotely, your institution shifts the possession as well as the control of that asset; it must rely on a response by the vendor, which likely provides a variety of technology assets to other customers with differing problems and priorities. Even when a technology asset is available and operating properly, the institution's users may need assistance.

While an on-campus IT team can choose to devote all of its available resources to resolve a particular problem with an installed technology asset, a cloud service vendor must allocate its available resources among different technology assets and in accordance with the different priorities of its multiple customers. Operating in the cloud, therefore, creates the risk that problems may not be resolved as quickly.

To manage that risk, review the obligations that the vendor offers to undertake to measure and maximize the availability of the service, resolve functionality errors, and assist users with their use of the service. Obligations of this type, typically called service levels, address six areas:

**Availability.** Availability refers to the percentage of time during a specified measurement period when the cloud-based service must be available for access and use by your institution's users. An availability service level of 99.5% is customary; mission-critical cloud computing services can carry service levels as high as 99.99%. The percentage is calculated by subtracting the time during the measurement period when the cloud-based service is unavailable from the total time during the measurement period, then dividing the result by the total time in the measurement period.

Examine a vendor's proposed availability calculation by identifying the proposed measurement period, measurement unit, and scheduled downtime allocation. The customary measurement period is a calendar month, with availability measured in minutes. Depending on the technology asset, the vendor may specify maintenance windows—periods of time during which the vendor is entitled to suspend services without penalty. Such suspensions, often referred to as "scheduled downtime," should have two components: specified maintenance windows and minimum advance notice (especially if, for example, maintenance windows last longer than a few hours' duration on one or two days per week). Minimum advance notice periods are negotiable.

**Error correction.** Technology errors range from serious malfunctions that interrupt business operations to minor annoyances. Neither the institution's IT team nor a cloud services vendor expects to provide the same type of response to errors of different severity. Errors are customarily ranked by levels of graduated severity (serious, moderate, and minor, for example), and response by a cloud services vendor should be appropriate for the severity level of a particular error. Because no one can reasonably promise to resolve a particular error within a specified amount of time that is reasonable, vendors often specify the level of effort they will expend at each level of severity (such as 24/7 or during business hours). After verifying that

# MANAGING THE RISKS OF OPERATING IN THE CLOUD

a prospective vendor has committed to resolving errors, compare those commitments to your IT team's historical resolution of errors related to that same technology asset.

**User support.** Users often have questions about accessing and using a particular technology asset. If your institution is considering a cloud operation for a technology asset that supports a large number of users, the vendor may assume the institution will provide primary user support, with the vendor answering only those questions posed by a small number of designated and trained support personnel. User support service levels may include average and/or maximum times within which responses to support requests are provided, the percentage of support requests resolved by the vendor's initial response, and the percentage of support requests resolved within a specified period of time.

**Service level measurement and reporting.** Together with your CIO, examine how the vendor proposes to measure its achievement of service levels and report the results. Many vendors, for example, require their customers to identify and report instances in which their service fails to achieve contractual service levels. If that's the case, you may not be able to assess the vendor's performance unless your IT team has the appropriate tools or other resources for doing so. Your institution might reasonably expect a vendor to measure its performance at each service level it offers and report the results each month.

**Performance incentives.** Typically, failure to achieve a service level leads to a service credit—an amount the institution may apply to future payment obligations to the vendor. Service credits are most effective when they reduce a vendor's profits. They should not cause the vendor to incur operating losses that could force cuts in operating costs and further impair the vendor's ability to deliver functional and reliable services. When charges for cloud services are payable monthly, the institution should be entitled to apply service credits to payments for the following month. When payments are annual—or service credits are attributable to service level failures during the final month of a contract—service credits should take the form of a refund.

Technology escrows may be offered as a remedy in Software as a Service (SaaS) transactions. The remedy typically requires two escrow accounts: one for object code and another for source code. The escrow agreement for object code should provide for release of the deposit upon a vendor bankruptcy, cessation of business, discontinuation of services, or a specified failure to meet an agreed-upon availability standard. Upon a release of the deposit, the customer can install and operate the applicable software in its own facility or that of a third-party hosting services provider. The escrow agreement for source code should provide for release of the deposit upon a vendor bankruptcy, cessation of business, discontinuation of services, or a specified failure to meet an error correction standard. Escrow provisions must be precisely drafted to be enforceable under U.S. bankruptcy laws.

A vendor's failure to meet promised availability, error correction, and user support service levels would breach the service agreement. However, the cure period in most contract termination provisions, unless modified, would deprive the institution of the opportunity to terminate the services agreement as a result of a failure to achieve service levels. Thus, consider an additional incentive for cloud services vendors to meet service levels. Specifically, your institution should seek a right to terminate the agreement without a cure opportunity if a critical service level is not met or if service levels are not met in a specified number of consecutive months (or a larger specified number of non-consecutive months).

**Technology changes.** One touted advantage of operating in the cloud—automatic and prompt updates to and replacements of technology assets—also creates risks. Technology updates and replacements inevitably change the way the technology performs, which may not be entirely welcome. Some automatic updates may even reduce functionality or require your institution to retrain users and/or modify its business processes. Changes to a cloud-based data processing application, for example, may necessitate changes to other installed interfaces that rely on the same data.

## SAFETY AND SECURITY ISSUES

You and your CIO should determine whether a proposed move to the cloud will transfer any confidential or protected personal information. This may include not only information about the institution and its development plans and finances but also data that third parties, such as research sponsors, have provided on a confidential basis. Although FERPA, HIPAA, GLB, and the ever-growing list of federal privacy laws often define protected information differently than state laws and regulations, most definitions cover all information from which an individual can be identified.

Certainly, your institution will want to safeguard its confidential and protected personal information not only from unauthorized disclosure (confidentiality and privacy interests) but also from loss and unauthorized access and modification (data security interests). Before transferring any of your institution's confidential or protected personal information to the cloud, verify that the vendor has policies and procedures which will reasonably support the institution's confidentiality, privacy, and data security interests. A number of laws and regulations require your institution to complete such verification before transferring protected personal information to any subcontractor.

The loss of and unauthorized access to confidential or protected personal information that results from hackers or technology failures aren't likely to be considered breaches of a vendor's confidentiality obligations. Although the loss of protected personal information may subject your institution to civil penalties—and the costs of notifying credit monitoring services on behalf of people whose information has been compromised—the liability limitation provisions in most commercial contracts exclude the vendor's liability for loss and unauthorized disclosure, use, and modification of confidential information and protected personal information. With your general counsel, identify the remedies to which the institution would be entitled should the vendor breach any of these obligations.

In addition, determine whether a cloud service permits your institution to access and retrieve its data or, alternatively, to obtain its data promptly upon request, both during the term of the cloud services agreement and after its termination or expiration. Your CIO should identify the format in which the data will be made available or provided and verify that the format allows the institution to meet its

needs to process and use the data. Until interoperability and universal data standards are more readily adopted for cloud services, migration to a vendor's proprietary data format may create portability issues if your institution decides to change vendors.

## MEETING FEDERAL AND STATE REQUIREMENTS

When deciding to operate in the cloud, your institution cannot transfer its responsibility to comply with laws and regulations to the cloud services vendor. If the institution fails to comply with any law or regulation because of a vendor's act or omission, the institution is liable for that failure.

Among the laws and regulations most frequently implicated in cloud computing transactions are privacy and data security laws, federal and state laws and regulations, and rules of accrediting organizations that require recordkeeping and reporting. Institutions that are public companies must also comply with the Sarbanes-Oxley Act, which requires appropriate controls for security, accuracy, and reliability of the technology used to store and/or process data used in financial reports. As a matter of best practices, institutions that are not public companies may adopt policies similar to the requirements of the Sarbanes-Oxley Act.

As preparation for operating in the cloud, join your CIO and general counsel in identifying all federal, state, and accreditation requirements applicable to your institution that the proposed cloud-based technology implicates. Evaluate the risks that the cloud service may create for the institution's ability to remain in compliance. The cloud complicates this analysis because your data may be stored in multiple jurisdictions, potentially subjecting your institution to different regulatory requirements.

Also identify the liability to which your institution would be exposed for failure to comply with the identified requirements, then evaluate the vendor's obligations to perform in a way that enables the institution to comply. For example, if your institution must meet the requirements of the Sarbanes-Oxley Act, or if it does so voluntarily, vendor obligations to conduct periodic SAS 70 Type II audits are customary. The CIO and general counsel can also help you verify that the vendor's documentation and data preser-

# MANAGING THE RISKS OF OPERATING IN THE CLOUD

vation obligations would enable your institution to comply with electronic discovery obligations should litigation or an investigation arise.

## QUESTIONS TO ASK TO EVALUATE RISK

Before entering into an agreement for cloud computing services, use the following questions to help determine your institution's risk in these areas:

### Vendor's Risk Profile

- If the cloud services failed, how serious would the consequences be?
- Do the proposed services accommodate your institution's needs and business processes? Are they compatible with the institution's installed technology?
- Is the vendor financially stable?
- Are other customers receiving similar services from the vendor generally satisfied with the services?
- Does the vendor's agreement address the risks of operating in the cloud in an acceptable manner?

### Vendor's Reliability and Performance

- Does the vendor offer a reasonable availability service level and formula for calculating availability?
- How do the vendor's error correction service levels compare with your institution's correction of errors in installed technology assets?
- Will the vendor or your institution's support personnel be responsible for providing user support?
- How do the vendor's user support service levels compare with the service levels to which your institution's users are accustomed?
- Is the vendor obligated to measure and report its service level performance?
- Do the remedies offered by the vendor for service level failure create sufficient incentive for the vendor to achieve its service level commitments?

### Confidentiality, Privacy, and Data Security

- Do the proposed services require transfer of confidential information or protected personal information to the cloud?
- Does the vendor have policies and procedures that will reasonably support your institution's confidentiality, privacy, and data security interests?
- What remedies are available to your institution if confidential or protected personal information is lost or improperly accessed, modified, or disclosed?
- What are your institution's rights to access and recover data that have already moved to the cloud? When may these rights be exercised, and will the data be returned in a format that your institution can use?

### Policy and Compliance

- How will the proposed cloud services affect your institution's ability to meet applicable federal, state, accreditation, and electronic discovery requirements?
- What remedies are available if a vendor performance failure causes your institution to violate a federal, state, accreditation, or electronic discovery requirement?

Source: Philip D. Porter and Michael E. Larner;  
[www.hoganlovells.com](http://www.hoganlovells.com).

*Philip D. Porter is a partner and Michael E. Larner is a counsel in the Northern Virginia office of Hogan Lovells, an international law practice with offices in 44 cities. Porter leads Hogan Lovells' technology transactions and outsourcing practice groups in the United States and may be contacted at [philip.porter@hoganlovells.com](mailto:philip.porter@hoganlovells.com). Larner focuses on information technology, open source software, and commercial transactions for education clients and may be contacted at [michael.larner@hoganlovells.com](mailto:michael.larner@hoganlovells.com).*