Making the Decision to Contract for Cloud Services:
Managing the Risk of an Extreme Form of IT Outsourcing

Eric K. Clemons  |  The Wharton School  |  clemons@wharton.upenn.edu
Yuanyuan Chen  |  National University of Singapore  |  discy@nus.edu.sg

Abstract
Cloud computing is a form of outsourcing, and as such it shares the essential risk profile of all outsourcing contracts concerning opportunistic behavior, shirking, poaching, and opportunistic renegotiation. Cloud computing is also an advanced technological development effort, and as such it shares all of the risks of large and uncertain development efforts; it also shares the essential risk profile of all development efforts, where for a variety of reasons success cannot be ensured. These include functionality, political, project, technical, and financial risks. Standards for cloud computing may reduce many of the risks of opportunistic behavior on the part of vendors. Standards efforts cannot mitigate most of the development risks of cloud computing; no amount of legislation or standardization can make it possible for firms to do that which they could not have done, or that which is indeed algorithmically or computationally infeasible. Fortunately, most of the risk management techniques of outsourcing remain applicable in the cloud.

1. Introduction

This paper is about outsourcing cloud computing services. Outsourcing is by now a well-studied subject, but cloud computing is such an extreme form of outsourcing that it appears to raise new concerns. We suggest that since cloud computing is a form of outsourcing, the elements that contribute to its risk profile are the same as those associated with any other form of outsourcing. Likewise, cloud computing is also an aggressive new advance in online, web-based computing, and since it is a novel combination of technologies it will likewise appear to have a new set of risks associated with it. However, this is, in the end, just another advanced technology development effort, and the elements that contribute to its risk profile will be the same as those associated with any other advanced development effort. While the forms of risks associated with cloud computing may not be different, the sources of those risks and the relative weighting of concerns in the analysis of cloud computing decisions may indeed be different from those associated with previous, and now better understood, outsourcing decisions.

We understand traditional outsourcing of facilities, of business processes, even of software development. Under facilities management outsourcing a vendor could be responsible for virtually all hardware, and for support, operations, help desk, and other support functions. But we have seldom contemplated outsourcing of everything — infrastructure, development platforms, security and back-up, even software development — to a single party. In a cloud computing relationship, hardware, software, backup, operations, and help desk operations, are transferred to the cloud vendor, but with software as a service and platform as a service, much of software development and even control of the platform that enables software development are also transferred to the cloud vendor. And yet cloud computing adoption is an increasing trend in IT spending. In the first half of 2009, the adoption of cloud computing jumped 320 percent [28]. The spending on cloud computing is expected to reach 30% to 40% of IT budget in the next three years.

In order to make cost-effective cloud computing decisions that adequately protect against risk it is necessary to understand what cloud computing is, what its risk profile is now and in the near term, how standards affect those risks now and in the near term. Then, and only then, can the firm assess its objectives and its strategy for cloud computing.

The structure of this paper is as follows: Section 2 reviews what cloud computing is and why it has become attractive now. Section 3 reviews the contracting and development risks associated with cloud computing, in the context of the risks of more traditional outsourcing. Section 4 reviews the unique legal risks associated with cloud computing. Section 5 reviews the critical role of cloud standards and

---

reviews how standards can reduce the risk profile of cloud computing. Section 6 reviews the status of standards at present. Section 7 reviews the major components of cloud contracts. Finally, section 8 presents our conclusions concerning managing the risks of cloud computing.

2. What Cloud Computing is and Why it is Emerging Now

2.1. A description of cloud computing

As noted above, cloud computing is an extreme form of technology outsourcing.

Its first, and perhaps most basic, component is **Infrastructure as a Service**. Infrastructure as a Service, or IaaS, has its roots in the virtualization technology of the first decade of the 21st century. Rather than specifically assign applications to machines, as was the case on Wall Street before the loss of data centers during the 9/11 attack, the entire computing facility of a firm was viewed as a collection of servers, running a collection of virtual machines, on which jobs could be assigned as needed. With most of the computing world moving towards X86-based processors, from laptops to mainframes, the next logical extension is to have remote server farms provide virtualization services rather than obtaining them in-house. As Mike Zisman of IBM used to say about on-demand computing, “the central limit theorem is our friend!” By that he meant that the larger the vendor, the smaller the variance in their expected demand. Any large cloud computing vendor can already expect to have larger demand than most users, and as even large users move towards the cloud ultimately any cloud vendor can expect to have more demand than any user. This means that cloud computing offers the most efficient allocation of computing resources. This is different from timesharing because it is not for casual individual usage or for non-computationally intensive clients, but indeed is now being approached as an IT delivery mechanism for the most sophisticated and technology-intensive businesses.

The cloud’s second component is **Software as a Service**. Software as a Service (SaaS) entails replacing purchase or lease of software, generally operated on the client’s site, with pay per usage (person-hour, transaction volume, or other measure) generally operated in the cloud or on the vendor’s site [27]. Again, this is different from timesharing in the 1970s in which clients might use software on a timesharing vendor to perform unique data retrieval operations or specialized modeling. The software envisioned in SaaS may be core to a business’s operations, encompassing HR, accounting, ERP, or other essential processes.

Perhaps more novel, the third element is **Platform as a Service**. In Platform as a Service environments (PaaS), vendors provide not only infrastructure and software, but a proprietary development platform. While PaaS may greatly accelerate software development and deployment, it may also lock users in to the services of a specific vendor, since vendor’s development platforms will differ, and hence software suites developed on one cloud vendor’s platform may or may not operate properly in the environment of other vendors.

These elements, IaaS, SaaS, and PaaS, when combined with online internet access, provide the technology needed to generate cloud computing. There are numerous definitions available for cloud computing, but they are all largely equivalent.

- Cloud computing must provide dynamically reconfigurable on-demand capacity allocation, initiated by user, enabling the efficient provision of IaaS. This is often called self service provisioning, but more accurately should be called self-initiated provisioning.
- Cloud vendors often offer PaaS, SaaS, or both, in order to complement the instantaneous provision of necessary hardware with greatly accelerated deployment of necessary software
- Pay as you go, or pay per usage, replacing purchase or lease of hardware and software
- This enables the shifting of capital expenses to operating expenses, since nothing is purchased or leased, nothing is treated as a durable purchase, and everything is treated as a consumable resource
- And it greatly increases flexibility, reducing or eliminating the lost time waiting to obtain capacity if growth is significantly faster than anticipated, or conversely the time and expense needed to eliminate unneeded capacity if growth in demand is far slower, or capacity requirements even decrease.

2.2 Why is cloud computing interesting now?

Many of the elements of cloud computing have been available for some time. IaaS is a lot like remote time sharing of the 1970s, and software as a service has been available from time sharing vendors for as long as there have been time sharing vendors. And yet, everything has changed, the economics of

---

2 Personal communication.
hardware, the technology of software development, the cost of software development, even the role of software development and hardware acquisition for small and medium enterprises and for start-up businesses even within larger firms.

The economics of hardware are such that the first year cost of floor space, power, heating and air conditioning exceed the acquisition costs for hardware. Likewise, the cost of systems administration personnel (Sys Admins) greatly exceeds the cost of the servers they manage in most enterprises. Cloud computing enables a firm to pay the fully loaded costs — hardware, power, heating and cooling — only for the time they actually require their machines, which greatly rewards load leveling through cloud computing. More importantly, but less well understood outside the computing community, is the massive reduction in the expense of Sys Admin personnel. A small shop may require a Sys Admin for 10 servers. A large shop may be able to use one Sys Admin for every 1,400 servers. A huge and highly automated operation like Google’s or Amazon’s cloud services may be able to leverage one Sys Admin for every 10,000 or even every 100,000 servers, with an expectation that even another order of magnitude of improvement is possible. Cloud computing also changes the economics of hardware deployment by reducing the secondary and indirect expense associated with idle capacity and by automating server management. In brief, cloud computing offers even the smallest firms significant economies of scale in all aspects of their hardware expenditures, reducing both capital and operating expenses.

Additionally, SaaS allows many firms to avoid software development entirely and to use standard packages. More novel is the fact that PaaS changes the way firms develop their own service, greatly accelerating software development and reducing software development expenditures. Once again, these effects will be most significant for the smallest firms.

It has long been true that the indirect costs of hardware dominate the direct costs, and that the non-hardware costs (software and personnel) of computing dominate the hardware costs. We now see that cloud computing reduces both. IaaS reduces hardware costs and SaaS and PaaS reduce software costs.

Reduced costs are not enough for the emergence of cloud computing; the technology necessary for the implementation of the cloud must also be credible, and indeed it is becoming widely accepted. Thus, for the first time the environment is such that cloud computing is not only desirable but possible. Two trends, both well advanced, support cloud computing.

- We see the widespread acceptance of common infrastructure in users’ data centers: The X86 architecture has been almost universally adopted for processors, from smaller servers deployed in massive server farms as well as the largest corporate mainframes, and most run Linux or Microsoft operating system, with some form of virtualization hypervisor.
- Likewise, we see the nearly universal penetration of high-speed internet, based on LANs and WANs, and increasingly on WiFi remote access as well.

Interestingly, the element of cloud computing that most captured the popular imagination is the idea that since everything is online somewhere, everything is in the cloud, and since everything is in the cloud, everything is available through cloud computing. Two elements were essential before everything in the cloud could actually be available in the cloud.

- The first is true semantic access. Database management went a long way towards allowing information to be accessed based on its description (the essence of relational query languages) rather than by its location. URLs and hyperlinks allow users to access anything for which they know the address (assuming they have access privileges) but they do not allow the user to find and integrate all information that resides online anywhere.
- The second is interoperability and cross-cloud integration. Individual clouds are at present more like separate islands of related access, or even separate archipelagos, but scarcely support full interoperability. Each cloud has its own footprint, but at present clouds are separate and their footprints vary greatly in size.

3. Traditional Outsourcing Risks Associated with Cloud Computing

The risks of cloud computing include the standard risks associated with any form of outsourcing. Surveys of users indicate that concerns for these risks are quite salient (IDC Enterprise Panel on Cloud Computing, August 2008):

- Users are concerned that they will be locked in, resulting in higher costs (concerns 6, 7, 8, on

---

3 These estimates were widely discussed and widely agreed upon at the recent Cloud Computing workshop in Singapore, CloudAsia2010, 2-7 May, 2010 http://cloudasia.ngp.org.sg/2010/conference.php.
cost, lock-in, and shortage of competition among major vendors)
- Users are concerned that they will lose control over essential data or over essential proprietary expertise (concerns 1, 7, on security)
- Users are concerned with under performance of critical tasks, especially those associated with protecting their data security and data integrity (concerns 1, 2, 3, on security, performance, and availability)

Each of these translates directly into one of the standard risks associated with traditional outsourcing.

### 3.1. Outsourcing Opportunism Risks

Outsourcing opportunism risks are generally seen to have their roots in three forms of deliberate, self-serving vendor behavior.

- **Shirking and deliberate under performance** [1, 2, 4, 5, 6, 17]
- **Poaching and the theft of intellectual property, proprietary software, critical confidential data** [11, 5, 6, 8, 21, 23]
- **Opportunistic Repricing, Client Lock-in, and Vendor Hold-up** [5, 6, 7, 12, 13, 14, 15, 16, 24, 25, 26]

Each of these risks has slightly different forms in the cloud environment from those encountered in traditional outsourcing:

Shirking involves deliberate under-performance, while claiming full payment for services, and is enabled by information asymmetries. If the client were able to fully observe both vendor output and vendor effort, shirking would not be possible. The forms of shirking that will be possible in cloud computing contracts include (1) deliberate under-investment in server capability, creating slowdowns that can be blamed on the network rather than the service provider; (2) deliberate under-investment in back-up, dynamic firewall monitoring, and other data quality services that can detected only in the event of a breach of security, and (3) under investment in excess or spare capacity, which will be detected only in the event of highly correlated demand, due to anything from market crises, major shopping holidays, or focused denial of service attacks, which again would be undetected until the critical events occurred. We all know that airlines and other forms of public transportation cannot accommodate the peak demands associated with holidays such as Thanksgiving or Christmas, we know this well in advance, and we are able to stagger our travel accordingly. Local power grids understand that correlated demand, when commuters get home at the same time, ride their elevators, turn on their air-conditioners, and start cooking dinner, can lead to brown-outs but they try to provide sufficient reserve generating capacity, and users are not too badly inconvenienced unless the overload causes the grid to fail. It’s not at all clear how corporations would deal with digital brown-outs caused by unanticipated peak demand on cloud computing, in turn caused by market events or other events that lead to spikes in transactions.

Poaching includes misuse of data or of programs residing on the vendor’s site. It can entail making critical resources available to a competitor’s direct competitors, or providing them to vendors who will then do so; clearly, poaching entails the misuse of resources provided under contract, their use outside the terms of that contract, their use for the gain of the vendor, and their use in ways that harm the client. Other uses are less direct or less obvious, such as using resources simply to let a competitor of the client anticipate the client’s plan, or even to allow the vendor to anticipate the client’s renegotiation strategy with the vendor itself.

Opportunistic renegotiation is perhaps the greatest risk. While IaaS can be made reasonably safe, the other levels of cloud service provision are extremely vulnerable to vendor lock-in and subsequent opportunistic repricing. X86 hardware, Linux, and virtualization software / hypervisors are by now standard, and a client can more or less painlessly relocate to another vendor as long as the client maintains hot backup mirror images on his own site as well as can reliably regain possession of critical software and data in a timely fashion. SaaS and PaaS clients are more at risk. Indeed, to the extent that a client has developed unique applications based on a unique vendor platform, the client can no longer move his suite of applications to another vendor. Software developed on the Salesforce.com platform Force.com cannot readily be moved to a Google or Amazon cloud software development platform. What that suggests is that the protection of the market is illusory, and that the lack of interoperability at the higher levels of SaaS and PaaS create significant risks for the client due to the great possibility of opportunistic behavior by the vendor over time.

### 3.2. Technology Development Risks

Complex development projects and those that go beyond the technological norms of their times always create operational risks, both for the developer and for the client, due to the technical and operational limitations of the development effort. These risks are inherent in any complex development effort and are quite independent of risks that are motivated
by opportunism and pursuit of excess profits by the vendor. Since the opportunism risks associated with outsourcing are due to differences in incentives between client and vendor they can often be managed or mitigated by contract design. In contrast, the development risks associated with complex deployment of novel technologies, or technologies in novel combinations, are difficult to manage and unlikely to be managed solely by contractual mechanisms.

The list of risks is easier to identify than to manage [10]:

- **Functionality Risk** — Functionality risks arise when we do not know what systems will be required to do, or what they will be required to do over time as users and their requirements evolve [3, 4, 23]. We do not yet know entirely what capabilities will be needed in the cloud over the coming years. In particular, we do not know to what extent SaaS and PaaS will predominate, and therefore we do not know to what extent it will be increasingly difficult to integrate new applications with the existing legacy systems of the organization developed without proprietary PaaS. We do not know how different cloud vendors’ offerings will evolve, or what will be required to integrate applications developed by a single user, but in different cloud vendor environments. Likewise, we do not know what will be required to merge applications developed in different clouds as a result of corporate mergers or restructuring activities. In addition, we do not yet know how to provide full semantic integration and we do not yet know what forms of “data citizenship” will be required or how legislation will emerge on what data can and cannot be stored outside a country (e.g. France or Singapore) or outside an economic zone (e.g., the European Union). It is likely that laws in France will differ from those in the US or the EU, and vendors will need to implement systems that conform to a wide range of laws and regulations while still providing full backup including hot restart capability for online operational systems. Clients who commit to vendors who are unable to do a good job on the first run the risk of having access to only portions of the cloud. Clients who commit to vendors who are unable to do a good job on the second run the risk either of poor performance or inadequate compliance with the laws of their region.

- **Political Risk** — Political risks arise when members of the organization have reason to resist the proposed new development effort. This can be for any of a number of reasons, but most frequently involve job security, status, or compensation. Just as in most outsourcing cases [21], the move to cloud will, over time, render most of the local Sys Admin personnel redundant, and likewise may greatly reduce the number of in-house software developers required. While these personnel will ultimately become unnecessary, they remain essential at least briefly, and if they understand now that they will soon be terminated many of the best will leave for alternative employment as quickly as they can, and long before the client firm is ready to let them go. Just as the Chicago Mercantile Exchange, Merrill Lynch, and the New York Stock Exchange were very careful about announcing plans for electronic trading or reducing the role of pit traders, account executives, or specialists and floor brokers, all firms must now be careful to avoid actions that would cause their best staff to leave before the firms are able to disburse their responsibilities in the cloud.

- **Project Risk** — Project risks arise when the combination of technologies, or the scope of the development efforts, exceed the ability of developers to manage the implementation, to ensure adequate testing and thereby ensure adequate quality, or to ensure timely completion [11]. We can legitimately ask if any of the parties, either clients or vendors, really know how to perform the porting of applications to the cloud. Do they know how to ensure that the suite of applications will run properly while some are on the client’s site and some are in the cloud, and while some have been developed with traditional application development methodologies and some have been developed with the cloud vendor’s proprietary platform?

- **Technical Risk** — Technical risks arise when projects exceed the available capabilities either of hardware or software technology, or exceed the skills of the best available developers [17, 19]. Again, we can ask if there are unsolved technical problems, perhaps involving security and privacy, perhaps involving integration of applications developed on the client’s site with those on the vendor’s site that could make implementation of cloud computing more difficult than anticipated. Perhaps the only truly unbreakable security systems involve quantum computing, and they appear to be years or even decades away from widespread implementation.

- **Financial Risk** — Financial risks occur when projects fail to deliver expected benefits and in-
Cross border litigation is always problematic. Transactions on the cloud can potentially span many national borders, with a client in one nation, a vendor in another, the cloud data center in a third, and the internet service provider spanning numerous others. When cross-border wrongs (torts) are committed they may lead to cross-national litigation. Several elements of cloud computing may make cross border litigation in the cloud setting even more problematic.

- **Ambiguous performance measures may make it hard to detect problems or to assign responsibility to the guilty party:** If the end user’s service degrades is this the fault of the vendor, the net between the vendor and the client, a third party provider of software, or the user client’s own service measurement? The cloud will require standard and transparent measures of service level agreements and of transparent observation of the quality of all aspects and all components of service delivery.

- **Problems with misappropriation of data or programs:** First, litigation must occur in a jurisdiction with a legal system with strong respect for the rights of the owners of intellectual property. However, the avoidance of litigation requires adequate protection, to ensure that neither the vendor nor associated parties deliberately misappropriate valuable intellectual property or accidentally allows other parties access to this valuable intellectual property.

- **Problems with valuation:** If damages are assessed, the client needs a legal system that will assess damages commensurate with damage incurred in the client’s country, commensurate with client’s norms.

Cross border litigation is always problematic, but three-party litigation can be especially complicated. When the user of a service is based in one jurisdiction, the provider of the service is headquartered in a second, and their cloud is located in a third, litigation may become arbitrarily complex. The first and most fundamental issue is in what circumstances does a court have jurisdiction over a foreign defendant alleged to have committed a wrong in the cloud? The next issue is whether either contract party (either cloud vendor or client) selects the forum and jurisdiction when drafting a cloud contract, and indeed whether either party’s home jurisdiction — either plaintiff’s or defendant — honor the contract’s specification of jurisdiction if it is believed to be biased and unfavorable to the local party?

### 4. New Cross Border Legal Risks

#### 4.1. Cross Border Litigation

There is increasing concern in the US, the EU, Singapore, and other venues, about where data on their citizens is allowed to be stored and accessed [Section 505 of the USA Patriot Act, the EU Data Protection Directive 95/46/EC]. Of course, it has long been unclear what some of these restrictions mean — if data about a French citizen is stored on a facility located in France, and accessed from an account or a server with a French net address, but the individual performing that access is located outside France, have French and EU laws on data domiciles been violated? Presumably the laws will be written so that they cover the location of the client company and the vendor, but not the location of individual users; that is, current ambiguity will survive. But even this level of restriction will be difficult to enforce. Some cloud vendors do not provide locations in all venues, and some do not permit clients to specify the location of their data. Some have due diligence procedures that require multiple copies to ensure security, or caching to ensure performance, and it is not yet clear how users can specify data locations or can ensure that their specifications are followed.
5. The Role of Standards in Reducing The Risks of Cloud Computing

5.1. The Impact of Standards on Shirking Poaching and Opportunistic Renegotiation

As is well known [1, 5, 6], shirking is heavily dependent upon information asymmetry. If standards ensure that the vendor’s behavior is observable, if performance measures are clear, transparent, and unambiguous, and if the nature of every performance lapse can be unambiguously traced either to vendor failure or external failure, then service level agreements can be enforced and one aspect of shirking is no longer a cause for concern. If standards likewise ensure that security, integrity, and data backup procedures are transparent and routinely monitored, then another aspect of shirking associated with cloud computing can be managed. The third and final element, reserve capacity, almost requires government regulation, just as banks and insurance companies are required to maintain adequate financial reserves; competitive markets do not adequately reward the maintaining of idle or reserve capacity.

Like shirking, poaching is a problem only if it cannot be detected and punished. With adequate standards for the storage and subsequent audit of the full history of data access it should be possible to ensure that online resources — online programs and data — are not accessed by third parties. It is less clear how standards can ensure that data copied for archiving and security purposes are not abused.

Williamson’s term for opportunistic renegotiation or vendor holdup was “post contractual small numbers bargaining” and he noted that the problem was enabled by “idiosyncratic” or “relationship specific investments.” What that means is that opportunistic renegotiation is only possible when the client’s initial commitment to a vendor becomes unbreakable over time, allowing the vendor almost unlimited opportunities for repriicing in the future. Standards for the transfer of applications and of data from one vendor to another would ensure that holdup does not become a problem. The more a client is dependent upon the offerings of a specific vendor the more entangled the client becomes and the greater the vendor’s freedom to engage in opportunistic behavior. In particular, proprietary SaaS programs, with proprietary data formats, make transfer back to the client’s own shop difficult. Even applications developed by the client’s own personnel, but developed on a vendor’s proprietary PaaS platform development offerings, may be impossible to port to a new vendor, contributing to lock-in and the possibility of holdup and opportunistic repriicing.

5.2. The Impact of Standards Functionality Risk, Political Risk, Project Risk, Technical Risk, and Financial Risk

It’s not immediately obvious how standards can reduce most of the risks associated with the development of cloud ventures. Standards might help make it clear what the cloud would and would not be able to provide, reducing the functionality risk associated with reliance upon the cloud. Standards will not help deal with the political risk created by key personnel who know that they will soon be made redundant, and who leave before the organization is able to deal with their departure. Standards, properly designed for interoperability among cloud vendors, may help ensure interoperability between applications on the cloud and applications on a client’s site. This would help reduce the project risk associated with phased transition from client-based applications to cloud-based applications, and would help clients manage shops that included the integration of both client-based and cloud-based applications. While standards themselves will not address the problems caused by technical implementation difficulties within the cloud, to the extent that standards define what is required standards may reduce the technical risks of vendors’ efforts to implement their cloud offerings. Likewise, standards themselves will not reduce the financial risks associated with cloud-based implementation. However, to the extent that standards reduce the risks associated with using SaaS and PaaS, standards may make cost benefit analyses more favorable to cloud-based implementations.

6. Status of Standards Activities

Standards activities are under way in most major technologically advanced nations. There are activities led by governmental bodies, NGOs, and industry associations. In addition to participating in these activities, leading technology vendors — both current cloud vendors and outsourcing firms that hope to gain significant cloud market share — are fighting in what can best be called the cloud standard wars. IBM joined alliance with dozens of companies including AMD, Cisco, Fujitsu, HP, Intel to form the Open Cloud Standards Incubator Leadership Board. IBM wants an open standard for its own competitive reasons, as does Microsoft. In contrast, other cloud pioneers, now well established vendors, such as Google and Salesforce.com seem opposed to the open standards. It appears that their competitive

4 “IBM leads call for open “cloud” standard”, by Jim Finkle.
strategies will be advanced by differentiated offerings and closed cloud platforms.

Industry associations are playing key roles and making progress in setting cloud standards. For example, The Storage Networking Industry Association (SNIA) has approved a standard for the Cloud Data Management Interface (CDMI) as a SNIA architecture standard in Spring 2010\(^5\). National Institute of Standards and Technology (NIST) is working on the definition of cloud computing. And Association for Retail Technology Standards (ARTS) provides guidelines for private cloud.

Paradoxically, despite the enormous concerns of potential cloud customers for lock-in, hold-up, and opportunistic repricing, almost no significant standardization efforts under way today are aimed at ensuring interoperability or portability among competing cloud vendors.

7. Major Components of Cloud Computing Contracts

From the client’s perspective, firms should fully understand three general dimensions of cloud contracts: performance, security (including data citizenship and data residence (i.e., where data may be stored and where it may be accessed)), and legal recourse:

- **Performance**: Contracts should have a clear definition of service level requirements on (1) availability of services including uptime, support time, and response time; (2) system and network stability; and (3) service reliability and quality. In addition to the clear definition of service requirements, the contract should specify the disaster recovery plan and penalty for the service failure. Often, terms of current contracts are unacceptably disadvantageous to the client; for example, currently, most cloud contracts and service level agreements grant the vendor the right to terminate client’s right to get access to data at any time for any reason.

- **Security**: The second dimension addresses security, which relates to data ownership and access right, and is a form of protection separate and distinct from disaster recovery plans. Contracts should specify the client’s ownership of data on the cloud and limit vendor’s access rights to those absolutely necessary to provide services for the client. In addition, the contract should clearly specify the scope of data security protection and the penalty and the responsibility and liability of vendors in the event that a security breach does occur. In many current cloud contracts, data security is not guaranteed (e.g., Google Docs, Zoho, etc); the vendor is exempted from many of the responsibilities as a joint provider of the cloud service (e.g., Amazon Web Service). Another important contract clause, which is often ignored in outsourcing contracts, serves to regulate what happen to the data after service termination.

- **Legal recourse**: Legal recourse is related to how the contract parties resolve the disputes in the service delivery process. Legal recourse covers two areas: legal claim and evidence collection, and jurisdiction and forum selection. The right to file legal claims and rights to evidence collection should also be covered in the contract for cloud services. Currently both Google and Amazon place the responsibility on the customer themselves to claim for the service credit. The procedure for claims is quite tedious in the case of Amazon’s cloud contracts; claiming compensation for cloud outage requires that customers submit an email request containing evidence of the claim, including account number, dates and time of each incident including instance ids of all applications that were running and were affected during the time of each incident, and the customers’ own server request logs in order to document the errors and corroborate the claimed outage. Jurisdiction and forum selection refers to the contract clause(s) that determines how the parties will initiate any litigation resulting from the contract and which forum or jurisdiction will have authority. Currently, cloud vendors always specify a particular court in their preferred jurisdiction to hear any litigation matters arising in their provision of cloud services.

8. Conclusions

Our conclusions are direct and straightforward:

- Cloud computing is a form of outsourcing, and as such it shares the essential risk profile of all outsourcing contracts concerning opportunistic behavior.

- Standards for cloud computing may reduce many of the risks of opportunistic behavior on the part of vendors. Paradoxically, despite the
enormous concerns of potential cloud customers for lock-in, hold-up, and opportunistic re-pricing, almost no significant standardization efforts under way today are aimed at ensuring interoperability or portability among competing cloud vendors.

- Cloud computing is an advanced technological development effort, and as such it shares all of the risks of large and uncertain development efforts and the essential risk profile of all development efforts where for a variety of reasons success cannot be ensured.

- Standards efforts cannot mitigate most of the development risks of cloud computing; no amount of legislation or standardization can make it possible for firms to do that which they could not have done, or that which is indeed algorithmically or computationally infeasible.

- A good outsourcing contract is probably even more important in the cloud computing environment than it is for traditional outsourcing. Given the magnitude of the losses that can occur due to loss of intellectual property or breach of security, it’s also essential that the contract protect the client’s rights to litigate in a forum that is likely to be fair and unbiased, and likely provide fair and accurate valuation of any losses. The best contract, of course, is meaningless if the vendor is both unable to perform in accordance with the terms of the contract and unable to make adequate restitution. In cloud computing, like any other critical form of outsourcing, the vendor must be both technically and financially qualified.

Fortunately, most of the risk management techniques of outsourcing remain applicable in the cloud.

9. References


interpreting information technology sourcing decision from a transaction cost perspective: findings and critique”, Accounting, Management, and Information Technology, 5(3/4), 203-244.


