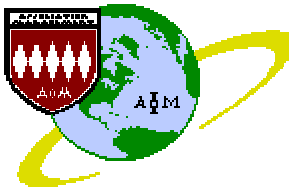

Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

GOVERNANCE AND SERVICE LEVEL AGREEMENT ISSUES IN A CLOUD COMPUTING ENVIRONMENT

MITCHELL COCHRAN
CLAREMONT GRADUATE UNIVERSITY
mcochran@ci.monrovia.ca.us

PAUL D. WITMAN
CALIFORNIA LUTHERAN UNIVERSITY
pwitman@callutheran.edu

ABSTRACT

The cloud computing environment provides for a new type of systems architecture. One key issue for a cloud computing client organization is to provide governance for data that it no longer directly controls. This paper identifies an initial set of guidelines to assist client organizations in defining governance plans for data they may choose to move to a cloud vendor. The client agency needs to ensure that data entrusted to outside resources is held to the same high standards as if the data were controlled internally. If there is a breach of security the vendor company may be legally responsible but the client agency may suffer the effects as well. The client agency needs to understand how its business practices will ensure compliance with industry standards such as HIPAA, PCI, and ITIL. Standard contractual arrangements such as service level agreements, confidentiality agreements, and PCI audits, among others, need to be extended to incorporate issues with hosting data in a cloud. This paper will investigate current research, and evaluate a cloud computing study that identifies proposed SLA attributes.

Keywords: cloud computing, governance, SLA, information security

INTRODUCTION

Cloud computing allows for organizations to move applications and data to remote servers. Similarly to discussions about virtual computing, cloud computing can provide for better utilization of resources. Hosted solutions and on-demand server resources are two examples where the use of outside vendors may provide for a lower total cost of computing. As the data is moved to remote resources, the governance or control of the data becomes a concern. Even though data may be hosted remotely, it is still an organization's responsibility to provide for its protection. The issue for the organization is to determine what mechanisms it has to provide for the protection of data which it may no longer directly control.

Cloud Computing Definitions

The European Network and Information Security Agency (ENISA), developed a working paper based on security features of cloud computing [3]. The definition that ENISA created is built on recommendations from the US National Institutes for Standards and Technology (NIST) [21], the Vaquero definition [24], and others:

"Cloud computing is an on-demand service model for IT provision, often based on virtualization and

distributed computing technologies. Cloud computing architectures have:

- highly abstracted resources
- near instant scalability and flexibility
- near instantaneous provisioning
- shared resources (hardware, database, memory, etc)
- 'service on demand', usually with a 'pay as you go' billing system
- programmatic management (e.g., through WS API)".

The NIST working definition includes many of the same common aspects of cloud computing [16].

- Characteristics: on demand self-service, broad network access, resource pooling, rapid elasticity and measured service.
- Deployment models: private clouds, community clouds, public clouds and hybrid clouds
- Service models: Software as a Service, Platform as a Service, and Infrastructure as a Service.

Further, Vaquero [24] defined three service model types of Cloud Computing – Infrastructure-, Platform-, and Software-as-a-Service (IaaS, PaaS, and SaaS). IaaS includes the provision of raw computing and storage services; while PaaS provides computing and storage along with specific platform software (e.g., the Google App Engine, a Linux/Apache/MySQL/PHP (LAMP) stack, etc. SaaS includes the provision of application software as an alternative to locally run applications (e.g., Google Docs, SalesForce.com).

Nicholas Carr wrote in *The Big Switch* that 100 years ago companies abandoned their own power generation and started plugging into the newly created grid [2]. The use of computer resources may be at the same type of junction point. As virtualization technology matures, high speed communications have higher penetration and administrators feel comfortable that they don't have to have the data on site, the use of cloud computing for resources will increase at a significant rate. There are benefits to the cloud similar attributes to those of using an electrical grid. In the case of the electrical grid, the services have become standardized. End user equipment has become standardized and accredited by independent authorities (Underwriters Laboratories, CA, etc.). The electrical grid infrastructure is monitored by a government body. As some point, it would not be unrealistic to think that there will be an independent monitoring service such as Cloud Audit (www.cloudaudit.org). The last attribute is that end users just 'plug in and go.'

Computer Industry Trends

The Gartner Group has identified a number of trends for the computing environment in 2010. In the 2010 CIO Agenda they identify that organizations need to move from efficiency goals to productivity goals. A Gartner survey of CIOs showed that virtualization moved from the third priority in 2008 to the top priority in 2009 [7]. Cloud computing made a more dramatic rise from number 16 in 2008 to the second place in 2009. Cloud computing provides a way for organizations to stretch budgets by taking advantage of efficiencies afforded by cloud computing. Gartner predicts that budgets will be flat in 2011 and 2012, and therefore organizations will need to prolong the life of aging assets while supporting new growth in requirements.

Gartner predicts the growth of cloud computing by including two end user predictions for 2010 which are: [13].

- By 2012, 20% of businesses will own no IT assets.
- By 2012, India-centric IT service companies will represent 20% of the leading cloud aggregators in the market

Organizations may have a financial incentive to accept cloud computing: "Cloud computing, which abounds with opportunities to shift IT resources outside the enterprise, boost liquidity and rebalance short and longer term financial commitments" [8]. Organizations are able to move from a capital purchase model for systems and applications to (commonly) a recurring fee based on usage. Gartner also points out that organizations will need to focus on strategic processes which provide competitive advantage. They need to be separated from those that provide competitive parity [8]. They go on to predict that organizations that integrate utility and cloud-based offerings in select business areas will gain a competitive advantage. The new processes will require strong risk management practices.

Gartner also predicts that the organizational support structure will change. Many engineers will learn new skills to optimize the cloud environment, but the number of hands-on infrastructure technicians and in turn administrative managers and direct supervisors will be reduced [13].

Despite these rosy projections, we realize there are limits to the acceptance of cloud computing, particularly in larger enterprises. Hofmann and Woods [9] claim that the acceptance of cloud environments will drop as enterprises get larger, due to issues of data portability, interoperability, and ability to customize. They further propose that private clouds might help to resolve some of

those issues. While the market and the evolution of technology will eventually sort those issues out, we still anticipate the need for organizations of many sizes to need to consider how best to manage or govern their data in the cloud, whether public or private.

Khajeh-Hosseini et al, discuss a number of governance issues for the cloud computing environment [11]. The authors point out that IT departments may move from a provider function to that of a expert for arbitration or certification, compliance departments may not have the same access to internally hosted systems and to consider if there are political implications if an organization loses control of its data. Schadler states that 'The IT department could serve as the leading tech adviser to an agency while the cloud handles the dirty work' [1].

The European Network and Information Security Agency (ENISA) identified that customers are just as responsible for the protection of their data as a host is. [3] Customers must realize and assume their responsibility as failure to do so would place their data and resources at further risk. In some cases cloud customers have inappropriately assumed that the cloud provider was responsible for, and was conducting, all activities required to ensure security of their data. The customer assumption, and/or a lack of clear articulation by the cloud provider places unnecessary risk on the customer's data. It is imperative that cloud customers identify their responsibilities and comply with them.

On its face, moving data to a cloud environment still requires the same fundamental security planning and attention as would be required in an on-premise environment, such as that identified in the McCumber Cube [25]. This model calls out the need for attention to issues of confidentiality, integrity, and availability, along with the need to secure data during processing, transmission, and storage. This is done by addressing issues of policy, education, and technology.

Beyond these common issues, a cloud computing environment can create opportunities for new types of issues, specifically in terms of human-created attacks. These cloud environment attacks can be classified into three general categories. The goal of the guidelines is to mitigate the effects of any one of the attack types:

- Attack on a hosted application in a SaaS environment;
- Attack on a hosted server in a PaaS or IaaS environment; and
- Attack via a trusted network connection to attack either from the client to the host, or from the host back into the client environment.

In a cloud environment hosted application, the applications are both hosted and owned by a separate party. In a hosted server solution, the owner of the application and the owner of the server can be two separate parties. The third situation is one where the connection is the target not the application or the server.

RESEARCH QUESTION AND STRATEGY

Seeing the impending growth of cloud computing in many sorts of computing environments, we anticipate changes to IT management practices due to the change in IT architecture. Given these trends, we seek to answer the following question: As IT managers seek to manage the introduction of cloud computing into their operating environments, what impact does this have on their governance practices beyond the traditional computing environment? The study will summarize what governance aspects that the participants feel are the most valuable. It will also summarize what industry changes will occur in the near future which will also affect governance methods.

The topic of cloud computing is still evolving and the discussion of definitions, frameworks and assumptions has not settled into industry standard practices. The goal of this paper is to develop and validate governance attributes for the new environment of cloud computing. The validation effort would require the opinion of experienced IT managers. The Delphi method which was developed by the Rand Corporation in the 1950's allows for developing a reliable consensus from a group of experts. [6] [17]

The Municipal Information Systems Association of California, MISAC, is comprised of IT managers from cities and special districts within the state of California. Municipal IT managers have exposure to a number of different business functions such as finance, human resources, public safety and time critical applications, process specific applications such as water or other utility control systems. The exposure allows for them to develop a broader level of expertise than IT managers from other types of small organizations. The members of MISAC work for cities with a population that range from 10,000 to cities larger than 2 million. The IT staffs range in size from a staff of two to over one hundred. The MISAC community is very active in discussing cloud computing topics so the members do have preliminary ideas for governance structures or attributes.

The specific participants were self-selected from a survey request to the MISAC listserv. The participants

of the two surveys were not identical but where from the same general population.

ELEMENTS OF CLOUD COMPUTING GOVERNANCE

Nondisclosure vs. Confidentiality Agreements

In our preliminary discussions of this topic among city CIOs, many used the terms 'nondisclosure' and 'confidentiality' agreements interchangeably. This common use infers that a nondisclosure agreement is equivalent to a confidentiality agreement. Craig Steele, City Attorney for the City of Monrovia, describes the legal distinction between these two as follows: a nondisclosure agreement requires that the signatory not overtly disclose the information, whereas the confidentiality agreement dictates that the signatories have a responsibility to protect the information [22]. If a vendor that has signed a nondisclosure agreement has a security breach, they would not be considered at fault for any disclosure. If a breach happens at a vendor that has signed a confidentiality agreement, the vendor would be responsible for the results of the security breach.

Legal location

As the real estate slogan goes, the three most important things about real estate are location, location, and location. From the user point of view, the location of a server on a network with broadband speed does not matter. From a legal point of view, location matters. The legal jurisdiction for a criminal matter would be where the vendor's server is located. A civil issue can span across jurisdictions. If there is criminal break-in to a vendor, the penalties would be based on the local jurisdiction of the vendor. If data moves to an off-shore site as a result of the theft, United States laws may not have any effect [22].

A civil matter, on the other hand, can be handled across jurisdictions. Business contracts can be stipulated to be litigated in either the vendor site or the client site.

One of the key areas of interest is the disclosure of compromised data. The issue is whether a hosted application vendor or a client organization is responsible to notify people that their personal information has been compromised. If a hosted financial application is based in a state other than California, for example, the vendor might not be liable to notify California residents under California state law. The legal question is if the vendor companies would be liable since the client is in California. The vendor is doing business in California so they would be liable under California law. In a similar way, the State of California is using this argument to collect sales tax from many companies that ship materials ordered over the Internet into the State. Any given situation would need to have legal experts examine the particular circumstances [22].

The issue will need to be handled by contractual arrangements. The agreement should require the host company to be financially responsible to notify all people that have had compromised personal information. There can be a significant cost involved in contacting all of the affected parties. The logic of the assumption is that the host company controls the data and access to the data. The client does not have any input on how the data is handled. If that data has been compromised, the host company may or may not be at fault but will have the contractual burden for notification. The host may chose to notify the affected people or may pay for the costs of the client to perform the notification.

Software License Restriction

There is a concern for software licensing in cloud computing environments. Daryl Plummer points out in his blog an issue in which license restrictions from purchased software may be violated when hosted on remote hardware [19]. Other software restrictions such as software or hardware keys may also pose a problem in remote environments. Some applications are keyed to processor serial numbers. As an application is moved, the processor serial number may change.

User-initiated security exposures

Security exposures can be created when end users post information to websites. Depending on how the site holds its data, there may be times, however brief, that data may not be fully protected. The organization needs to review and understand every part of the process. If a security exposure is found it needs to be mitigated to the lowest reasonable level. The following is a simple example.

- Step 1 – A user posts personal information on website using a secured session
- Step 2 – The client organization gets a notice that data has been posted and retrieves it using a secured session

The issue is that there is a brief time that data may reside on a remote host. The SLA would need to verify what administrators have access to the data, and if there are logs that are retaining personal data. What is the assurance that it is secured according to legal standards?

A second user-initiated exposure is the self deployment of cloud based applications. As paths are created for acceptable cloud applications, users may deploy additional unscreened applications. Many cloud based applications can be self deployed without the screening of the internal IT organization [12]

Connections to Remote Services or Networks

One of the benefits of cloud computing is to be able to integrate SaaS resources applications into an organizations internal applications. As a matter of course the connection should be protected to provide for data security in transit. The concern can arise that the SaaS provider's network security is unknown. The remote network may have become part of the local network. In so doing, the local network is at risk for any security deficiencies in the remote network. [23]

Many organizations take advantage of a single security sign-on. Depending on the configuration of a remote resource the single sign-on may option may not be available. The two organizations may or may not be able to develop a trusted relationship.

PCI Security Standards Council

The Payment Card Industry, or PCI, has implemented a Security Standard Council. The council developed Data Security Standards (DSS) for organizations that store, process or transmit cardholder data. The guidelines are enforced by the major credit card companies: Discover International, Visa, MasterCard, American Express, and JCB International. The Council has suggested that security is an ongoing process. The organization needs to assess, remediate, and report on the security. The Security Standard Council has developed twelve standards for version 1.2, presented in table one. [18]

As part of the contract or Service Level Agreement (SLA), the vendor would need to verify that PCI standards are followed. Most of the suggested procedures cannot be independently verified by the client. The vendor would need to attest that the correct procedures are being followed. The client organization could request an independent company perform an audit but there could be a large cost involved. The vendor might be able to spread the SAS70 Type 2 audit costs across their entire client base.

Table 1: PCI Security Standards

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

Assessment

There is an assessment program identified by the PCI-DSS that describes both Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). The ASV performs vulnerability scans of the Internet-facing interfaces of the merchants and service providers. It would be one added level of assurance to have a report from an ASV.

PCI-DSS provides guidelines for cardholder data elements. Cardholder data such as primary account number (PAN), cardholder Name, Service Code, Expiration Date can be stored with protection required. The vendor is not to store the authentication. If sensitive data from the magnetic strip is stored it is required to be unreadable. That data could include the full magnetic stripe data, CAV2/CVC/CW2/CID and PIN/PIN Block.

When data is transmitted, strong cryptography is required which could be SSL/TLS or IPSE. The host needs to implement a need-to-know basis for their employees. There is no way for each client to independently verify what controls the host has in place.

Brian Prince [20] lists seven security risks with cloud computing. :

- Abuse and Nefarious Use of the Cloud- can be anonymous registration of users
- Insecure API's – Interfaces need to have strong authentication, encryption and access controls are in place
- Malicious Insiders - require transparency into the provider's information security and management practices
- Shared technology issues – not designed for isolation, need to review logs
- Data loss or leakage – need strong key management, storage and destruction practices
- Account or service hijacking – block sharing credentials between users and services
- Unknown risk profile - Security by obscurity may be low effort, but it can result in unknown exposures.

The security risks point to the common need that data and transactions need to be encrypted or protected at all times. For example, some simple web application use email as a transport mechanism. There is a security issue concerning confidentiality in both transport and storage operations. Procedures or a SLA would need to address the following areas:

- Has the email been encrypted?
- If the data is stored in a database on a server that is accessible to the Internet, how long until it is moved to a secure location?
- What are the security precautions relating to the database?
- Is the data stored in an encrypted format?
- If stored in a database on a server that is accessible to the Internet, how long until it is stored, it does not matter how long.
- How is the database protected?
- How is data backed up? Even if the data just transitions across a server, it may hit the point that a backup is taken.
- What information is kept in transaction logs?

ENISA [3] recommends that the vendor should have a set of standard security controls which include:

- firewall
- IDS/IPS (Network and Host based)
- system hardening and in-house penetration testing
- ITIL compliant incident and patch management.

The ENISA study also points out an issue for the cloud computing vendor. The vendor may receive data from the client that the client may not have obtained by lawful means. A vendor may be responsible for data that is uploaded to it [3]. The ENISA study also points out the issue of lawful access by law enforcement. While data is protected from unauthorized access, it may also need to be made available for legally required access.

A virtual server security issue may also apply in a cloud computing environment. The issue is if applications from a guest partition can hack into the host partition. [14] If one virtual server is hacked, can the compromised server be used to attack adjacent or shared servers?

EXTANT PROPOSALS APPLICABLE TO CLOUD GOVERNANCE

U.S. National Institute for Standards and Technology (NIST)

The NIST bulletin on Telework Security focuses on recommendations for securing communications [21]. The bulletin's recommendations are very similar to those in the PCI-DSS standards.

- Plan telework security policies and controls based on the assumption that external environments contain hostile threats. '
- Develop a telework security policy that defines telework and remote access requirements.
- Ensure that remote access servers are secured effectively and are configured to enforce telework security policies.
- Secure telework client devices against common threats and maintain their security regularly.

Information Technology Infrastructure Library (ITIL)

ITIL provides for five disciplines within its definition of service delivery. The five disciplines include: service level management, capacity management, IT service contingency planning, availability management, and financial management for IT services [15]. McPhee points out that the SLA enables that IT service provider and the customer will have a clear understanding of the expected level of services and the associated costs. ITIL identifies a number of issues for client service level management within the definitions of ITIL:

- make sure that the vendor fulfils the requirements of the SLA
- provide a service catalog,
- provide for service continuity

A number of ITIL Service Management Planning sub-activities may directly impact a cloud computing environment:

- Create a security section for a SLA: This process contains activities that lead to the security agreements paragraph in the service level agreements. At the end of this process the *Security* section of the service level agreement is created
- Create underpinning contracts: This process contains activities that lead to underpinning contracts. These contracts are specific for security.
- Create operational level agreements: The general formulated goals in the SLA are specified in operational level agreements. These agreements can be seen as security plans for specific organization units.
- Reporting: In this process the whole Create plan process is documented in a specific way. This process ends with reports.

The ITIL news blog site points out a contractual difference in that underpinning contracts may include financial penalties where the SLA may just be an agreement [10]

One of the major issues is whether the vendor company or the client is responsible for notifying a person that their confidential information has been breached. Many vendors write into the contract that they are not responsible. The ENISA study suggests a requirement that cloud vendors notify customers of data security breaches [3].

CloudAudit and the Automated Audit, Assertion, Assessment, and Assurance API (A6)

CloudAudit is an example of an organization that could take the role of an independent authority that sets the generally accepted operating procedures and security standards for cloud governance. The goal would be similar to that of Underwriters Laboratories does for electrical appliances in the United States. The organization is a volunteer cross-industry effort. The CloudAudit organizations goal is to provide a common interface that allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their infrastructure (IaaS), platform (PaaS), and application software (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology [4].

The organization defines their execution strategy as:

- Keep it simple, lightweight and easy to implement; offer primitive definitions & language structure using HTTP(S)
- Allow for extension and elaboration by providers and choice of trusted assertion validation sources, checklist definitions, etc.
- Not require adoption of other platform-specific APIs
- Provide interfaces to Cloud naming and registry services

CURRENT INDUSTRY PRACTICES

Many practitioners and academics have proposed recommendations for cloud computing procedures and controls. Preimesberger lists 10 mistakes that enterprises can make when starting to use cloud computing [19]:

- "Implementing an Infrastructure that Doesn't Fit Your Cloud Needs
- Not Verifying or Auditing the Security of Your Cloud-Based Provider
- Using Internet Bandwidth Inefficiently
- Not Having Backup and Disaster Recovery Plans
- Getting Trapped Paying Hidden Fees
- Not Knowing Where Your Data is Actually Kept
- Selecting a Vendor on Name Recognition Rather than Service Quality
- Failure to Establish a Process to Ensure Your Vendor Honors SLAs
- Ignoring Cloud Management
- Choosing Cost Over Service"

These identified areas summarize issues that have been raised by other authors. The goal of this research effort is to identify what legal, contractual, and procedural options should be considered by organizations before they move to cloud computing which will include:

- Standard service level agreements – uptime, access, cost, what security practices are followed, etc.
- Additional language – who is notified when a breach happens, what users and administrators can see what information (e.g., Health Insurance Portability and Accountability Act (HIPAA) or other legal restrictions)
- Indemnification

- Insurance
- PCI – Vulnerability Assessment (part of PCI methodology)
- Confidentiality agreement

DELPHI RESEARCH STUDY

The qualitative study was based on Delphi principles using California municipal IT directors and managers as the experts. MISAC is the Municipal Information Systems Association of California. MISAC member cities range from small cities with populations of 10,000 to large cities such as Long Beach, San Francisco, and Los Angeles. The majority of the respondents were IT managers of cities with populations of 40,000 to 100,000. The MISAC member participants were polled for the two survey phases of the study.

The first survey asked for the overall concerns and then issues that might arise for specialized environments. The first question asked for the participants' general initial thoughts. It was intended to get their preconceived notions on the topic. The later questions asked for thoughts or concerns given a series environments or situations. The intention was to stimulate thoughts about situations that the participants might not have considered. The survey asked for concerns about the following specific environments or situations:

- An application development environment
- Integration of dis-similar applications
- Server deployment
- Asset management
- Remote backup
- Security management of servers and how to control access to servers
- Audit / change management
- Testing or technology advancement
- Privacy or security concerns of a cloud computing environment
- If the participant envisions any legal issues or impacts due to the use of a cloud environment
- Factors or stipulations do they want to see in a cloud computing service or resource contract such as an SLA
- Any differences that the participant sees between a cloud computing and hosted applications
- What will the impact of Cloud computing be in the period of five to ten years in the future
- If any applications should be locally hosted

The first survey was answered by 14 IT managers. The replies were collated into a set of cloud computing attributes related to governance, and the list was edited to merge common topics with slightly different wordings. The completed list of attributes is shown below:

1. The vendor needs to demonstrate PCI compliance by providing details of the infrastructure
2. The vendor needs to provide a PCI complaint audit
3. The vendor needs to provide SAS 70-Type 1 audit: attestation of adequacy of controls
4. The vendor needs to provide SAS 70-Type 2 audit: includes on-site evaluation
5. The vendor will provide measures for E-Discovery
6. Indemnification clauses for the client organization will be needed
7. The vendor will need to provide statistics to gauge for SLA compliance
8. The vendor has identified which employees have access to cloud resources
9. The vendor has no access to customer data
10. Testing or audit procedures will be provided
11. The data will be encrypted during communications
12. The data will be encrypted while being stored
13. Transaction logs are only available to the customer that they pertain to.
14. The vendor has secondary sites for vendor disaster recovery
15. There will be priority schedule on how cloud resources are restored after an outage
16. The contract will include capabilities for migrating to a new vendor
17. The contract will include a sunset date
18. The vendor will provide information or controls on how data is moved to new locations
19. The vendor will allow changes to their update or patch schedule
20. The vendor will provide information on firewall and security configurations
21. The contract will include restrictions on rates or fee changes
22. The SLA will include discussions of liability for hacking or virus attacks.
23. The vendor will provide backup capabilities
24. The client organization can specify the backup schedule
25. Any backups are encrypted
26. The vendor is able to commit to five nines uptime

27. The SLA needs to provide for financial penalties for non performance
28. The SLA needs to provide for a test environment
29. Cloud resources can be authenticated to verify identity
30. The vendor will provide a private cloud environment

A second survey in the Delphi methodology is intended to rank the importance of issues raised in the first survey. It also gives the participants to add thoughts that might not have been raised in the first survey. The issue for phase 2 was for participants to rate the importance of the identified attributes for a cloud computing contract or environment. The participants rated the attributes on a 1 to 5 scale that was defined as:

1. No Value
2. Helpful
3. Significant
4. Essential – still negotiable
5. Critical – non negotiable

Both the first and second surveys drew participants from the same Information System manager population. The second survey had 27 participants. The results showed that 23 of the 30 attributes were rated as either essential or critical (scores 4 & 5) by 75% or more of the respondents. The remaining 7 items (marked with ** and ***) were rated as essential or critical by 50% or fewer respondents.

1. The vendor needs to demonstrate PCI compliance by providing details of the infrastructure
2. The vendor needs to provide a PCI complaint audit
3. The vendor needs to provide SAS 70-Type 1 audit: attestation of adequacy of controls **
4. The vendor needs to provide SAS 70-Type 2 audit: includes on-site evaluation ***
5. The vendor will provide measures for E-Discovery
6. Indemnification clauses for the client organization will be needed
7. The vendor will need to provide statistics to gauge for SLA compliance
8. The vendor has identified which employees have access to cloud resources
9. The vendor has no access to customer data
10. Testing or audit procedures will be provided
11. The data will be encrypted during communications
12. The data will be encrypted while being stored
13. Transaction logs are only available to the customer that they pertain to.
14. The vendor has secondary sites for vendor disaster recovery
15. There will be priority schedule on how cloud resources are restored after an outage
16. The contract will include capabilities for migrating to a new vendor
17. The contract will include a sunset date **
18. The vendor will provide information or controls on how data is moved to new locations **
19. The vendor will allow changes to their update or patch schedule ***
20. The vendor will provide information on firewall and security configurations **
21. The contract will include restrictions on rates or fee changes
22. The SLA will include discussions of liability for hacking or virus attacks.
23. The vendor will provide backup capabilities
24. The client organization can specify the backup schedule **
25. Any backups are encrypted
26. The vendor is able to commit to five nines uptime
27. The SLA needs to provide for financial penalties for non performance
28. The SLA needs to provide for a test environment
29. Cloud resources can be authenticated to verify identity
30. The vendor will provide a private cloud environment

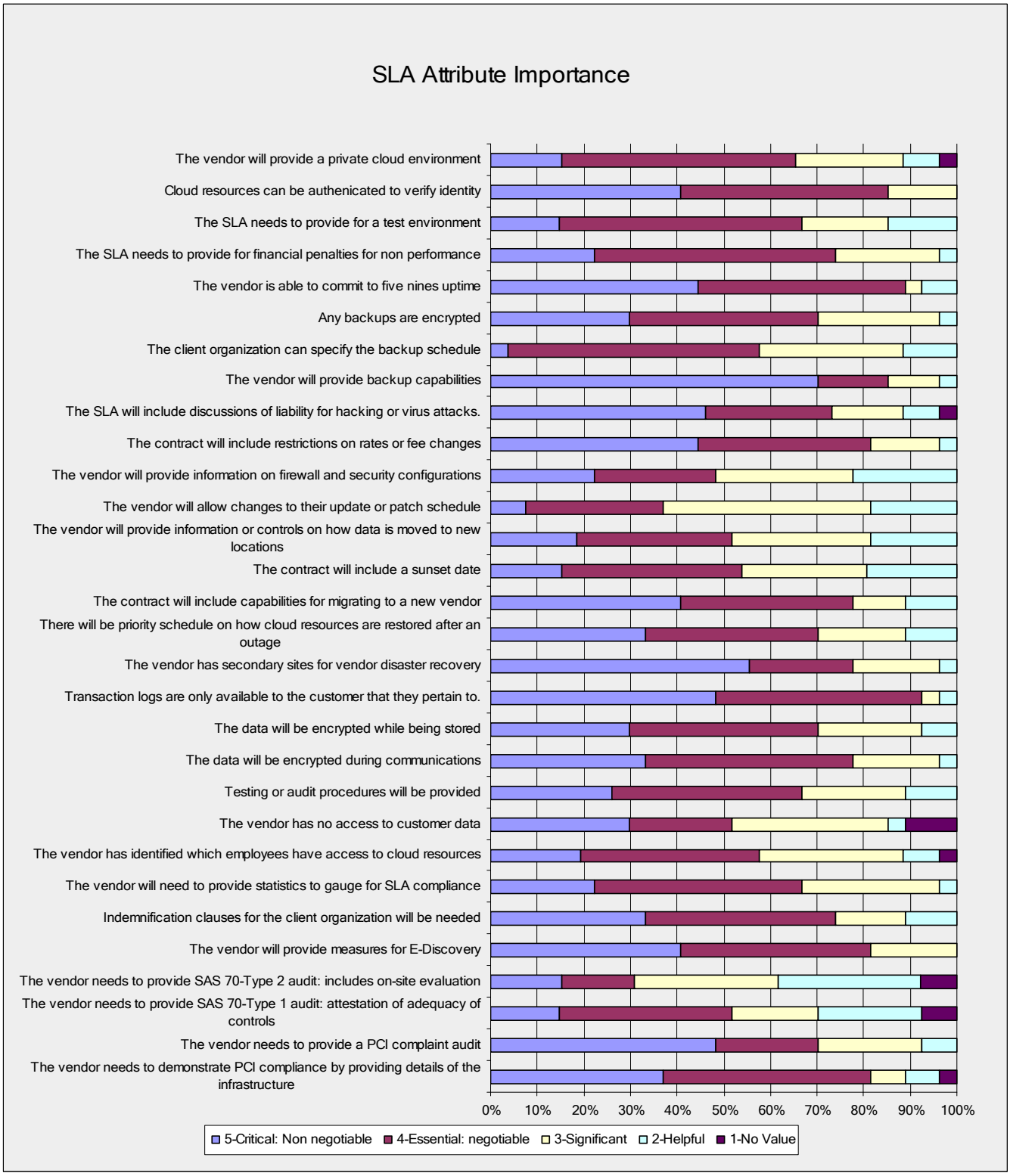

Figure 1: Survey Two Results

There were 5 questions which are marked with a '**' that were below that threshold. Those questions were scored as a '4' or '5' for approximately 50% of the responses.

- 3 - The vendor needs to provide SAS 70-Type 1 audit: attestation of adequacy of controls **
- 17 - The contract will include a sunset date **
- 18 - The vendor will provide information or controls on how data is moved to new locations **
- 20 - The vendor will provide information on firewall and security configurations **
- 24 - The client organization can specify the backup schedule **

Two questions marked with a '***' only scored at 25% and 17% respectively a '4' or '5'. However, those two questions still scored a majority of responses as significant or a '3'. The attributes are important but respondents felt that there would be room to negotiate. The first question asked for onsite verification. The second question requested for control of the patch schedule.

- 4 - The vendor needs to provide SAS 70-Type 2 audit: includes on-site evaluation ***
- 19 - The vendor will allow changes to their update or patch schedule ***

The second survey was also answered by MISAC members however there were participants in the second survey that did not respond to the first survey request. The second survey participants were asked to rate the findings of the first survey.

The second survey respondents were also asked to look to the future and what the impact of cloud computing will be on the industry over the next five years. Cloud computing can move the resources from inside the organization to outside the organization which will have an impact on the IT organization, roles, and mission.

The second survey had a larger response rate than the first survey request. The respondents were also MISAC members as in the first survey. The participants were asked to rate on a scale of 1 to 5 if they agree with the provided statements. Four questions marked with a '**' showed agreement but not as overwhelming as the other responses. The responses on those questions showed less than 50% agreement.

1. Current cloud computing environments have difficulty providing a thorough audit trail
2. Vendor reputation is more important in a cloud environment
3. Lost of control of the environment is an issue for trouble- shooting
4. Cloud-based applications will be harder to integrate **
5. Client organizations will need to provide redundancy in case of a short term Internet outage
6. Client organizations will need to provide redundancy in case of a long term application outage
7. Client organizations will need to provide local storage in case of an outage of any duration **
8. Future cloud computing could cause IT staffs to move from development to auditing skill sets **
9. Future cloud computing could cause IT staffs to move from development to integration skill sets
10. Your programming skills sets will have to change to meet the new environment
11. Most computing tasks will be in the cloud in the future **
12. Public safety applications should remain locally hosted.
13. Agencies will need redundant links to the Internet
14. E-Discovery procedures will be a critical component of a SLA

The second survey consisted of a summary of the results from the issues listed in the first survey. A critical component of the Delphi method is to gather additional issues during each survey phase. The second survey asked if there were additional issues that were left out of the summary of the first survey attributes. The second survey respondents did not add issues to the ones listed in the second survey. Since there were no additional issues, a third survey was not necessary.

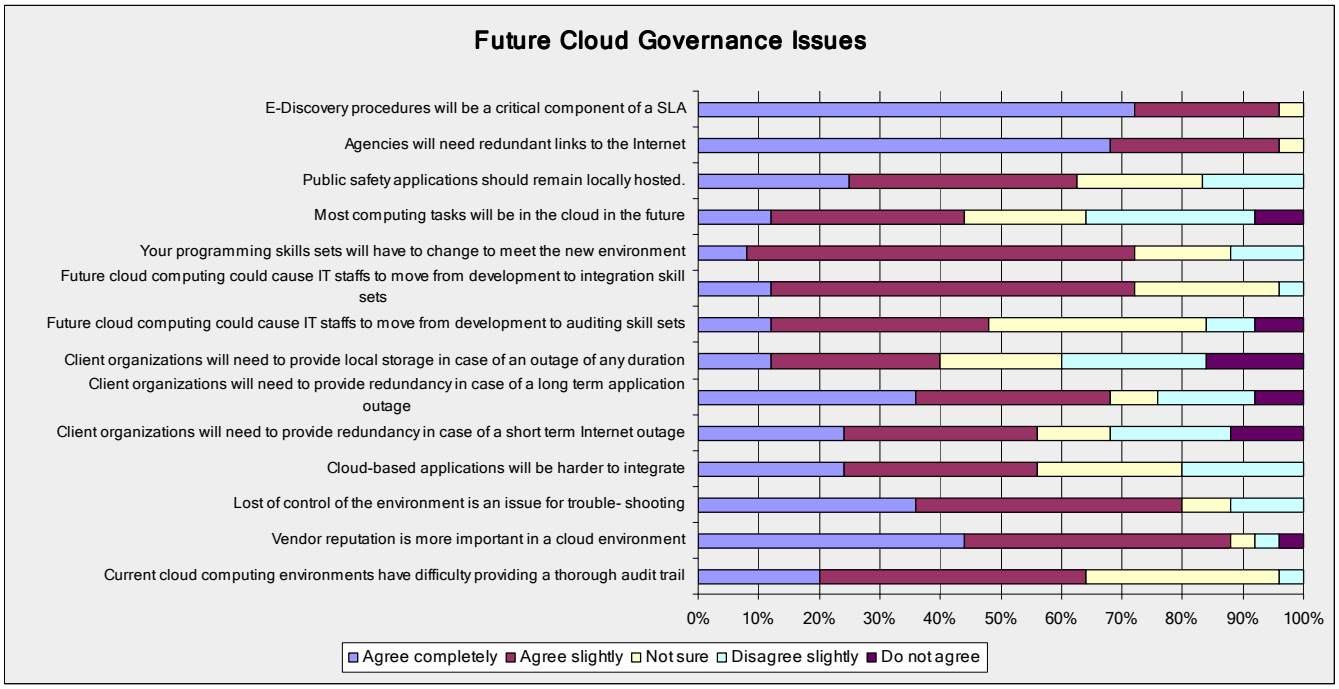

Figure 2: Anticipated Future Issues

Survey Discussion and Implications for Practice

The results show that the cloud computing environment will require additional attributes or functional requirements in a SLA beyond what is currently used today in a traditional SLA contract. The attributes specify tasks that would normally be handled internally as a normal part of the organization. Now that those tasks are being handled by an outside organization, there will need to be controls or standards put in place. The study shows that attributes developed in the study should be considered in any SLA in a cloud computing environment. The new attributes extend many common internal controls for use between organizations. For example, the SLA could require information similar to that of an internal audit from the outside vendor.

The future study questions show that cloud computing will have a profound impact on the IT organization. As applications are moved to the cloud, the IT organization may loose control for audit, security and or integration capabilities. The loss of those controls will require the organization to include the remedy in the SLA. Since the IT organization may not have control of application there may be issues integrating applications from different cloud vendors. One of the key questions was related to the cloud vendor's reputation. A concern is that it might be impractical to provide small test implementations to test how a vendor performs related to a SLA. Due to the somewhat invisible nature of the cloud computing environment it will be difficult to audit or even change vendors. The cloud computing environment provides a service but not the description of the underpinnings that create or support the service offering. The SLA and vendor provided environment define a relationship between the entities. If the environment is customized then it can difficult to change to new vendors. In the worst case, the organization needs to understand the steps that would be necessary to take back the applications from the cloud and host them internally. The reputation may be used as a critical decision point in selecting a vendor. Auditing and e-discovery will be primary concerns in the future as well.

The organization will also have to change some aspects of its mission. Many of the support functions will move to the application host. As other organizations are providing the application what is the role of IT. The key roles will be to be the technology advocate, support the local infrastructure and to provide integration of resources. The best response was an answer to the open

ended question of IT's organizational role in the future; it is to act as the 'fall guy' for problems

CONCLUSION

The paper discusses how computer governance measures will need to be updated to fit into a cloud computing environment. A set of initial recommendations have been developed based on computing standards such as NIST and COBIT. These recommendations are supported by a Delphi study which asked California municipal IT managers to identify and rank their concerns. The study provided the following contract attributes which should be considered in the development of any service contract for a cloud computing environment.

- Provide a company assessment and review what confidential information is required. The organization needs to understand what portions of the process have a risk. The risk could be in communications, storage, processing or backup.
- Required secured access with strong authentication for all communications
- Required encrypted communications
- Require a Service Level Agreement which includes:
  - Availability as needed: time/day of week/uptime
  - Upgrades / customizations
  - Require that the vendor follow NIST security practices
  - If possible, include financial penalties to increase the strength of the agreement. The recommendation includes the concept of an underpinning contract.
- Require a confidentiality agreement instead of a non-disclosure agreement
- Require indemnification agreements which allow the organization to outsource risk.
- Require a PCI assessment (where appropriate to the industry and data usage)
- Provide for a contract sunset or termination date
- Provide for an exit and transition strategy to allow for data and information to be moved to a new vendor.
- Identify which party will be responsible for any legal disclosures or remedies that will need to be given to affected parties.

One of the concerns for IT management is to prove that it has done its 'due diligence' in its efforts to protect the organization's information. These steps are supported by the findings in the study:

- Security needs to be end to end, not just each participant managing their shop or portion of the process.
- An organization's lines of business or communities of practice need to develop standards that are relevant to their needs. The processes need to be based on industry standard practices such as NIST, Certified Information Security Systems Professional (CISSP) and Control Objectives for Information and Related Technology (COBIT) criteria or 'books of knowledge'. For example the process should develop a periodic penetration testing criteria.
- Develop criteria for procedures that vendor and client each need to follow.
- Develop a new template service level agreement which includes a confidentiality agreement rather than a non-disclosure.
- Address any legal requirements that may be necessary. As stated previously, a confidentiality agreement would be preferable to a non-disclosure agreement.
- Data that is stored in a cloud might be stored anywhere in the world. Is there a legal requirement that data be maintained within the boundaries of a particular country?

The organization needs to identify the requirement and procedure in case of a disclosure of personal information. The state or country in which the organization hosts the data may have different disclosure laws. The client organization will need to determine procedures:

- to determine the extent of the disclosure
- to notify clients in case of disclosure

The normal SLA or contract components of an exit strategy also need to exist but are not directly related to cloud computing. The contract needs a sunset date with renewals periods. If the contract has become untenable, then it ends without penalty to either side. The exit strategy would also need to include access to data and information. If possible, the termination should include access to the program logic. Without an understanding of the logic, the data may be useless.

DIRECTIONS FOR FUTURE RESEARCH

The field will mature and standardized procedures will develop from commonly accepted practices.

The question is how to ensure that the field is level as to appropriately balance power, information and responsibility among clients and the hosts. Case law will develop as contract breaches by either the host or the client are litigated. The litigated procedures will help to develop generally accepted practices or standards.

Generally accepted industry practices such as the book of knowledge from either the Certified Information System Security Professional (CISSP) or Project Management Professional (PMP) help to set commonly accepted industry practices. Those practices are further refined for customized environments such as Windows by the manufacturer. Microsoft has developed standards and practices which are enforced by the Microsoft education and certification process. The organizations that promote standard practices need to evaluate how the unique elements of cloud computing might alter some of the current standards.

Future enhancements in security technology will allow for some additional protective measures. IBM has recently introduced an interesting technology where data can be manipulated without it being decrypted [5]. For a cloud computing environment, the data would be protected from being viewed or directly acted on by host server administrators.

REFERENCES

[1] Bernoff, J., and Schadler, T., *Empowered*, Harvard Business Press, 2010.

[2] Carr, N.G., *The Big Switch, Rewiring the World from Edison to Google*. 2008, New York: W. W. Norton & Company.

[3] Catteddu, D. and G. Hogben, *Cloud Computing - Benefits, risks and recommendations for information security* 2009, European Network and Information Security Agency: Heraklion, Crete, Greece. 125 pp.

[4] CloudAudit. CloudAudit.org home page; http://www.cloudaudit.org/, May 2010.

[5] Cooney, M., "IBM touts encryption innovation". Network World, http://www.networkworld.com/news/2009/062509-ibm-encryption.html, June 25,2009.

[6] Dalkey, N., and Helmer, O. An experimental application of the Delphi method to the use of experts, Management Science, 9 (3), pp458-467, 1963.

[7] Gartner Group, "Leading in times of transition, the 2010 CIO Agenda", in *Gartner Executive Programs*. 2010A, Gartner Group: Stamford, CT. 67 pp.

[8] Gartner Group, "Top End User Predictions for 2010: Coping with the new balance of power", in *Gartner Executive Programs*. 2010B, Gartner Group: Stamford, CT. 8 pp.

[9] Hoffman, P. , Woods, D. "Cloud Computing: The Limits of Public Clouds for Business Applications", *IEEE Internet Computing*, 1089-7801, Nov-Dec 2010, p90-93.

[10] ITIL News.com, ITIL Service Management, http://www.itilnews.com/index.php?pagename=service_level_management,, June, 2010.

[11] Khajeh-Hosseini, A., Sommerville, I., and Sriram,I., *Research Challenges for Enterprise Cloud Computing*, Cloud Computing Co-laboratory, University of St. Andrews, http://arxiv.org/pdf/1001.3257, 2010.

[12] Lundquist, E. CIO Strategy: the Private and Public Clouds Mashup, Baseline Magazine, December 2010, p 18.

[13] McGee, K., Harris, K, Morello, D., Raskino, M., Lopez, J., Prentice, S., *Predicts 2010: CIOs and IT Executives Brace for a Tough Year, Even as Economic Indicators Improve*. 2009, Gartner Group: Stamford, CTpp.

[14] McLaughlin, L.," Future Threats to Virtualization Security: Fact vs. Fiction", *CIO Magazine*, November 14, 2007.

[15] McPhee, D. *ITIL and Security Management Overview,* Information Security Management Handbook, Sixth Edition, Volume 2, edited by Harold F. Tipton and Micki Krause. New York: Auerbach Publications, 2008.

[16] Mell, P. and Grance, T. *The NIST Definition of Cloud Computing,* National Institute of Standards and Technology, 2009.

[17] Okoli, C. and Pawlowski, S., "The Delphi method as a research tool: an example, design considerations and applications", *Information & Management*, 42 (2004), pp 15-29.

[18] Payment Card Industry Security Standards Council, "PCI Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 1.2", https://www.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf, 2010

[19] Preimesberger, C., "Top 10 Mistakes Enterprises Can Make When Moving Data into the Cloud", *EWeek*, http://mobile.eweek.com/c/a/Cloud-Computing/Top-10-Mistakes-Enterprises-Can-Make-When-Moving-Data-into-the-Cloud-811577/, March 4, 2010.

[20] Prince, B., "Cloud Computing's 7 Deadliest Security Risks". *EWeek*, http://www.eweek.com/c/a/Security/Cloud-Computings-7-Deadliest-Security-Risks-345990/, March 12, 2010
[21] Scarfone, K., *Security for Enterprise Telework and Remote Access Solutions*. 2009, National Institute of Standards and Technology: Washington, DC. 7 pp.
[22] Steele, C., City of Monrovia, California, personal communication, 2010
[23] Thurman, M., "Security Manager's Journal, Tightening Up SaaS Security", *ComputerWorld*, December 6, 2010, p 40.
[24] Vaquero, L.M., et al., "A Break in the Clouds: Towards a Cloud Definition", *ACM SIGCOMM Computer Communication Review*, 39(1), 2009, pp. 50-55.
[25] Whitman, M., "Management of Information Security", *Course Technology*; 3rd edition, 2010, pp. 4-5.

AUTHOR BIOGRAPHIES

Mitchell Cochran is the Information Systems Manager for the City of Monrovia in California. He has served as President of the Municipal Information Systems Association of California (MISAC). He has a number of conference papers dealing with governance and E-Government.

Paul D. Witman is an Assistant Professor of Information Technology Management in the School of Business at California Lutheran University. Witman holds a Ph.D. in Information Systems and Technology from Claremont Graduate University. His research interests include information systems in non-profits, information security, usability, technology adoption and continuance, and electronic banking and finance.