CLOUD SERVICE PROVIDER MANAGEMENT

PROGRAM EVALUATION AND AUDIT

METROPOLITAN COUNCIL

November 2015

INTRODUCTION

Background

Cloud computing is defined by the National Institute of Standards and Technology as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services)." Cloud computing comes in various forms, known as models. These service models include near outsourcing of resources (Infrastructure as a Service), supporting in-house applications on a cloud service provider's platform (Platform as a Service) and using third-party applications run on the cloud service provider's infrastructure (Software as a Service.) Furthermore, cloud service can be private to one organization, shared by multiple organizations with shared missions, or open to the public. Each combination of service model and deployment model has a unique risk profile.

Use of cloud computing has expanded at the agency in recent years. Multiple business units have sought cloud-based solutions for operations while existing service providers have sought to move to a cloud-based service model. The benefits of using cloud services include flexible deployment of resources and potential cost savings. The risks include unclear responsibilities between service provider and client, security, data ownership, and the necessity of adequate controls.

Purpose

- Determine adequacy of contracts and contractual compliance between the service provider and agency
- Determine if internal control deficiencies within the agency and it's interface with Cloud Service Providers exists, and recommend solutions to mitigate or strengthen controls where necessary
- Provide an assessment of the effectiveness of the cloud service providers internal controls and security

Scope

Cloud providers were identified in collaboration with Information Services (IS). From this pool, a judgmental sample of nine current or expired contracts (covering eight providers) was selected for further review based on discussions of risk with IS staff. Contracts in the sample were executed between August 2013 and July 2014, with two exceptions; one contract was executed in July 2009 and included in the sample because issues were identified with the vendor, while the other was executed in October 2007 and was renewed via the 2013 sole source procurement for hardware and software maintenance. Contracts total approximately $1.6 million, and include cloud-based services for Regional Administration (7), Environmental Services (1) and Community Development (1).

Methodology

- Review of cloud service provider contracts
- Interviews with relevant staff from Information Services, Procurement, and Business Units
- Cloud service provider internal controls assurance questionnaire

Assurances

This audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and the U. S. Government Accountability Office's *Government Auditing Standards*.

OBSERVATIONS

Cloud services were purchased without the involvement of key information services functions during the requirements phase of projects.

Of the nine contracts reviewed, audit could confirm the involvement of information security during the requirements phase in one case, involving a provider administering an HR application. The involvement of information security in the purchase of the other cloud services in the sample could not be confirmed prior to the signing of the contract. The involvement of continuity of operations staff prior to purchase was confirmed only for the software used by their staff. The appropriate involvement of key Information Services (IS) functions, such as information security and continuity of operations staff, during the requirements phase of a project is necessary to implement the agency's information security policy. The information security policy states "Information systems belonging to the Metropolitan Council must be managed and protected so that confidentiality is maintained (preventing information from unauthorized disclosure), integrity is ensured (preventing information and systems from accidental and malicious modification), and availability is guaranteed (ensuring the reliability and accessibility of data and resources to authorized individuals in a timely manner.)"

Several reasons were identified for cloud services being purchased without the involvement of information security and continuity of operations staff. First, Information Services is not always aware of when contracts for IT-related services are initiated. When hardware and software is needed, an Information Technology Request (ITR) form is filled out, which informs IS of the need prior to purchase, among other things. The cloud services in the sample either went out for bid through the procurement process or were renewed through a sole source procurement. In each of these cases an ITR was not needed. A contract initiation memo (CIM), required to initiate a procurement over a certain dollar amount, was used instead per procurement procedures. The CIM does not have a mechanism to notify IS of IT-related services like the ITR does. There is a gap in IS being aware of IT-related services that are initiated through the CIM. As a result of this gap, involvement of IS in the procurement is driven primarily by the diligence of agency project managers who may not be aware of who to involve in the process, and involvement may occur after the requirements phase of a project. Second, a project manager reports that they work with IS staff assigned to their department, who were not aware of the need to work with information security or continuity of operations. Third, one project manager reports using the same RFP with minor changes as the previous time it went out, and did not think it needed to change. These reasons point to the need to notify IS when IT-related contracts are initiated, to clarify the role of key IS functions during the requirements phase of projects, and to communicate the role of key IS business functions to project managers and IS staff across the agency.

An additional effect of the inconsistent involvement of IS in these cases is that an inventory of cloud service providers and associated contracts could not easily be produced. A full inventory of systems containing agency data is necessary to monitor the effectiveness of information security controls.

Information security policies and procedures can be improved to support the management of cloud service providers.

The current information security policy was adopted on 03/25/2009, and six procedures flow from the policy. However, the procedures do not specify security standards or responsibilities in working with external parties who access the Council's information, nor do they address the assessment of risks posed by external parties. A checklist has been developed by information security to help guide the security requirements for cloud service providers. The checklist may be a basis for future security procedures, standards or as part of a risk assessment, but it has not been formally required or adopted as such.

Best practice guidance for the management of information security (ISO 27002) discusses the importance of risk assessment prior to working with external parties. It states, “Where there is a business need for working with external parties that may require access to the organization’s information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements.” This guidance suggests a risk assessment should be required in policies, procedures or standards for external parties.

Policies, procedures and standards for external parties and cloud service providers help ensure data security and continuity of operations risks are addressed consistently throughout the agency. These risks include compliance with data practices laws and maintaining access to critical data according to continuity of operations standards.

One of nine contracts included recommended contract language for cloud service providers; three of nine contracts included Service Level Agreements, two of which met recommended criteria.

A review of nine cloud services contracts was conducted for cloud-service clauses recommended by ISACA[1]. One contract satisfied 13 of the 15 criteria for cloud service contracts. It was notably missing an audit clause, but this was somewhat mitigated by requiring full disclosure of cloud service provider security policies and third-party performance audits of the vendors internal controls—two clauses that occurred in only one other contract. Seven of the remaining eight contracts included less than half of the recommended contract clauses. Three were considered “non-standard” agreements, which means they were provided by the cloud-service provider and did not follow one of the approved contract templates of the agency. These contracts showed variation in how many clauses were addressed. One included 9 of 15 of clauses, while another included only 2 and was missing an audit clause.

Two of the nine contracts had Service Level Agreements (SLA) that met recommended criteria. SLAs define acceptable service levels to be provided to the agency by the specific service provider. Service level agreements should reflect business, security and continuity of operations requirements, be measurable, include consequences for not being met, and be incorporated into the cloud service contract.

Difficulties with a specific vendor serve to illustrate these points. A vendor handling agency GPS data transferred part of its service to a third-party cloud service provider. When the contract term expired, information security reported difficulty getting agency data back from the third-party. The contract addressed the subcontracting risk by including language that the vendor cannot subcontract any part of the work without prior approval—that subcontracting occurred highlights contract administration and monitoring issues . The fact that the vendor did not originally provide cloud-based services would have made it difficult to anticipate and address specific cloud-based security risks in the contract, but in this case, the data security risks were similar for both the vendor and the cloud-based subcontractor. For example, recommended contract language for agency ownership of data, collection of third-party audit

[1] Formerly the Information Systems Audit and Control Association, ISACA is “an independent, nonprofit, global association…[which] engages in the development, adoption and use of globally accepted, industry-leading knowledge and practice for information systems.”

reports, and explicit expectations for how data is managed at the end of end of the contract would have helped address the data security risks illustrated by this vendor and its cloud-based subcontractor. The issues with this vendor served to raise awareness of data security and external vendor risks to Council management, and action was being taken to improve contract language at the time of the audit.

One of four cloud service providers could not provide evidence their internal security practices are followed.

A sample of four cloud service providers were selected for review to give increased assurance that their internal security practices were adequate to protect agency data. A questionnaire was sent to each service provider asking them to provide third-party audits of their operations, information security certifications or attestations, internal security policies and other operational questions.

One provider could produce a summary of internal security policies, but could not produce evidence of third-party audit reports or security certifications to demonstrate compliance with internal policies. (Appendix 1) A requirement to provide third-party audits was not in the contract, but an external audit was reportedly in progress. While the provider was cooperative in responding to the questionnaire, an audit clause was missing from this contract. Based on what was provided by the vendor, audit cannot confirm their adherence to their internal security practices without further auditing their operations.

One cause of this finding is that no documentation of monitoring of the contract or service levels could be produced for the contracts reviewed by audit. Monitoring processes and responsibilities between business units and IS are not defined, nor is a process to track and follow up on issues that arise with a vendor. Additional causes relate to the findings above. Lack of involvement by information security and agency security policies contributed to a contract with this vendor that did not include recommended language. As a result, the agency is limited in their ability to produce evidence that the vendor handles agency data appropriately and to hold them accountable if they don’t.

CONCLUSIONS

The governance and management of cloud service providers is an emerging issue for the agency as business units increasingly seek to take advantage of cloud-based service opportunities and existing vendors move to cloud-based service models. Governance and management functions can be improved by being more defined and integrated across business units, from appropriate involvement of Information Services during the requirements phase of projects, to the development of contracts and contract monitoring processes.

RECOMMENDATIONS

Program Evaluation and Audit recommendations are categorized according to the level of risk they pose for the Council. The categories are:

- **Essential** – Steps must be taken to avoid the emergence of critical risks to the Council or to add great value to the Council and its programs. Essential recommendations are tracked through the Audit Database and status is reported twice annually to the Council's Audit Committee.
- **Significant** – Adds value to programs or initiatives of the Council, but is not necessary to avoid major control risks or other critical risk exposures. Significant recommendations are also tracked with status reports to the Council's Audit Committee.
- **Considerations** – Recommendation would be beneficial, but may be subject to being set aside in favor of higher priority activities for the Council, or may require collaboration with another program area or division. Considerations are not tracked or reported. Their implementation is solely at the hands of management.
- **Verbal Recommendation** – An issue was found that bears mentioning, but is not sufficient to constitute a control risk or other repercussions to warrant inclusion in the written report. Verbal recommendations are documented in the file, but are not tracked or reported regularly.

1. **(Essential) Information security policies, procedures and standards should be reviewed and updated to provide management direction and support for the purchase of IT-related external vendors.**

   A risk assessment process prior to acquiring external IT services is recommended be included in policies or procedures.

   Management Response: *Information Services (IS) agrees that information security policies and procedures should be reviewed for updates to the security standards required to protect Council data stored and used by cloud service providers. Guidance needs to be included to mitigate risks identified prior to acquisition of external IT services.*

   Staff Responsible: *Dave Hinrichs (CIO) and Eirik Felter (Technology Security Officer)*

   Timetable: *Time must be provided to research necessary changes, coordinate with internal stakeholders, and follow the Council's review and approval process. Anticipated completion by the end of third quarter 2016.*

2. **(Essential) The role of IS should be reviewed and defined during the requirements phase of IT-related projects and throughout the procurement process.**

   Increased controls to better ensure appropriate IS awareness of IT-related contracts are recommended.

   Management Response: *The Procurement Department has modified its Solicitation Planning Package intake worksheets to ensure that IS is consulted on procurements of hardware and* *software systems. Cloud storage security language is one of the requirements that is evaluated.*

Staff Responsible: *Micky Gutzmann and Dave Hinrichs*

Timetable: *These intake worksheets have already been implemented. IS will consult with Procurement on any necessary changes as new needs arise.*

3. **(Essential) Use cloud service specific language in cloud provider contracts, including agreed upon security and continuity of operations requirements, and develop Service Level Agreements with cloud providers.**

   Where feasible, consider amending existing contracts with high-risk cloud service providers to include cloud-specific contract language.

   Management Response: *The Procurement Department, Office of Legal Counsel and IS-Security staff have developed contract language that will be included in agreements which involve the sharing or creation of Council data. We agree this language needs to include continuity of operations requirements and that service level agreements should be negotiated into agreements that involve private not public data and/or support of critical/high priority services.*

   Staff Responsible: *Micky Gutzmann and Dave Hinrichs*

   Timetable: *Implementation is planned for end of first quarter 2016. Identification of high risk cloud service provider contracts requiring amendment will be difficult and likely require the full year to implement.*

4. **(Significant) IS should define contract monitoring responsibilities and internal issue tracking processes for external IT services.**

   Responsibilities should also be communicated to relevant staff. The following monitoring and tracking processes are recommended:

   - Periodic collection and review of third-party security audits unless otherwise determined by a documented risk assessment.
   - Logging issues in a centralized system.
   - Process for monitoring the provider identified as not demonstrating adequate assurance of internal security practices.

   Management Response: *Contract monitoring responsibilities for external IT services requires more attention than it has been given, especially with more focus on external cloud services. Providing more active contract management is time consuming and without dedicated staff focused on this function, it does not receive the attention it deserves due to the press of business in IS to keep systems running effectively and efficiently Council-wide.*

   IS management will work with Executive management to determine how to effectively implement improved monitoring and tracking processes, and the type of staffing that is necessary to implement this recommendation.

   Staff Responsible: *Dave Hinrichs, Pancho Henderson and Sue Hauge*

Timetable: *Since it will be necessary to inventory and identify that all cloud service IT service contracts have the necessary contractual language to ensure that security, continuity of operations and service level agreements are in written form, this recommendation will not be completed until the end of 2016.*

5. **(Significant) An inventory of all cloud service providers across the agency, with associated service level agreements and contracts should be created.**

   Procurement, IS and business unit representatives should collaborate in developing the processes for creation and maintenance of the inventory.

   Management Response: *We agree that an electronic inventory of the Council's cloud based services needs to be created, and Procurement and IS will collaborate with business partners on how to best develop, create and maintain this inventory.*

   Staff Responsible: *Pancho Henderson and Sue Hauge*

   Timetable: *End of third quarter 2016.*

Appendix 1: Cloud Service Provider Questionnaire Results

Criteria	CSP 1	CSP 2	CSP 3	CSP 4
Audit rights in contract?	N	Y	Y	Y
Received questionnaire?	Y	Y	Y	Y
Received third-party audit reports?	N, will send when complete	Y	Y, cover page	Y
Received CSP internal security policies?	Y	Y	Y, “PCI"	Y
Received certifications or attestations?	N	Y, PCI	Y, PCI	N
Adequate evidence of CSP internal security processes?	N	Y	Y	Y

Appendix 2: Relation of audit recommendations to Thrive MSP 2040 principles

Recommendation	Integration	Collaboration	Accountability
1			X
2			X
3			X
4			X
5			X

METROPOLITAN
COUNCIL

390 Robert Street North
St Paul, MN 55101-1805

651.602.1000
TTY 651.291.0904

public.info@metc.state.mn.us

metrocouncil.org