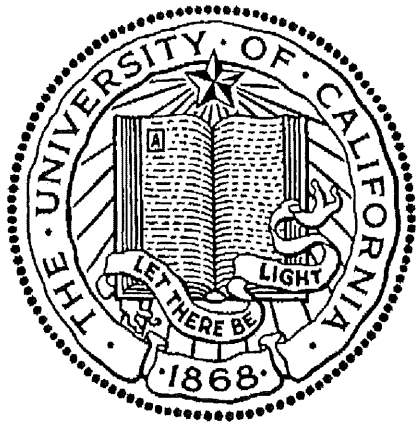

AUDIT AND ADVISORY SERVICES

Cloud Computing
Audit
Project No. 15-643

July 14, 2015

Prepared by:

Chad Edwards
Auditor-in-Charge

Reviewed by:

Jaime Jue
Associate Director

Approved by:

Wanda Lynn Riley
Chief Audit Executive

UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
Tel: (510) 642-8292

611 UNIVERSITY HALL #1170
BERKELEY, CALIFORNIA 94720-1170

July 14, 2015

Larry Conrad
Associate Vice Chancellor for Information Technology and Chief Information Officer
Office of the Chief Information Officer

Associate Vice Chancellor Conrad:

We have completed our audit of cloud computing as per our annual service plan in accordance with the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* and the University of California Internal Audit Charter.

Our observations with management action plans are presented in the accompanying report. Please destroy all copies of draft reports and related documents. Thank you to the staff of the Office of the Chief Information Officer, Campus Shared Services, Educational Technology Services, and Information Security and Policy for their cooperative efforts throughout the audit process. Please do not hesitate to call on Audit and Advisory Services if we can be of further assistance in this or other matters.

Respectfully reported,

Wanda Lynn Riley
Chief Audit Executive

cc: Executive Vice Chancellor & Provost Claude Steele
Vice Chancellor John Wilton
Senior Vice President and Chief Compliance and Audit Officer Sheryl Vacca
Associate Chancellor Nils Gilman
Assistant Vice Chancellor and Controller Delphine Regalia

University of California, Berkeley
Audit and Advisory Services
Cloud Computing

Table of Contents

OVERVIEW

Executive Summary

Audit and Advisory Services (A&AS) completed our audit of cloud computing as part of our annual service plan for fiscal year 2015. The purpose was to provide management with an objective assessment of the effectiveness of internal controls for identifying cloud service providers and analyzing requirements prior to solution acquisition to ensure that cloud service providers meet campus requirements (including review of costs, benefits, and risks) as well as for the ongoing monitoring of performance. The scope of the audit involved reviewing a sample of three contracts with the cloud service providers Google, Instructure, and ServiceNow.

The campus has a contract with Google for the use of their email (bMail), calendar (bCal), word processing, spreadsheet, slide presentation, storage and collaboration (bDrive), and video chat (Google Hangouts) productivity tools. Educational Technology Services has a contract with Instructure for the use of their learning management solution that offers instructors (1) the ability to build a site, (2) a diverse set of communications tools and (3) the capability to create and manage assignments and grades. Campus Shared Services has a contract with ServiceNow for the use of their service management automation suite for requesting IT service (i.e., service request ticketing system), incident management, and problem management.

While the evaluation of cloud service providers generally follows similar practices for the procurement of other services by the campus, internal controls for analyzing requirements, including analysis of costs and risks, and whether service providers satisfy our requirements before acquisition are minimally effective. Due diligence procedures need enhancement to include, for example, analyzing the cost of alternative delivery models and service providers;, evaluating the risk that the service provider may not continue to operate, and obtaining assurance the service provider is capable of meeting our security, availability, privacy, and information process requirements. In the absence of these procedures, opportunities to increase cost savings may be lost, service providers may not possess the capabilities to safeguard our data, the campus may engage a service provider where there is substantial doubt about the service provider's ability to continue to operate, or service provider's standard terms and conditions may not meet campus requirements.

Once service commences, control activities also need strengthening to ensure cloud service providers continue to perform as agreed, meet future campus needs, and provide competitive pricing. There are gaps in the measures of performance and the reporting of those measures to aid managing supplier performance. For example, measures focusing on service usage, user satisfaction, changes to the service (including changes in cost), as well as for ensuring on-going conformance with our security, privacy, availability, and processing integrity needs are currently minimal. The responsibility for regular and formal reporting by cloud service providers is unclear in the contracts we examined, potentially impacting effective contract management. In the absence of these provisions, while cloud service providers may meet our requirements at the time of acquisition or be the best alternative, there is no guarantee they will continue to meet our requirements through the term of the contract or continue to be the best alternative for meeting our needs in the future.

Source and Purpose of the Audit

A&AS completed our audit of cloud computing as part of our annual service plan for fiscal year 2015. The purpose was to provide management with an objective assessment of the effectiveness of internal controls for identifying cloud service providers and analyzing requirements prior to solution acquisition to ensure that cloud service providers meet campus requirements (including review of costs, benefits, and risks) as well as for the ongoing monitoring of performance.

Scope of the Audit

In planning this audit, we obtained an understanding of campus risk management and control processes, applicable laws and regulations, the types of risks that could have a significant effect on the use of cloud computing, and prior audit engagements. We performed a risk assessment and made a preliminary evaluation of controls for purposes of determining the areas, timing, and the extent of audit work to perform.

Audit techniques included reviewing a sample of three contracts with cloud service providers (Google, Instructure, and ServiceNow) and evaluating documentary evidence and verbal descriptions about how the provider selection process operates.

Background Information

The university has a systemwide agreement with Google for the use of their productivity tools by any of the ten campuses. The Berkeley campus subsequently amended this agreement by attaching additional security provisions and restrictions on the physical location of where data can be stored by Google. The productivity tools deployed as a part of the campus' implementation includes email (bMail), calendar (bCal), word processing, spreadsheet, slide presentation, storage and collaboration (bDrive), and video chat (Google Hangouts). Information Services and Technology manages the service, which went live in a phased manner beginning in May 2013 and finishing in June 2013.

The campus has an agreement with Internet2 for Canvas, a learning management solution provided by Instructure. Internet2 is a non-profit organization that serves the research and academic community by acting as a broker between cloud providers and cloud consumers/tenants. Instructure utilizes Amazon Web Services for hosting Canvas. Canvas offers instructors (1) the ability to build a site, (2) a diverse set of communications tools[1], and (3) the capability to create and manage assignments and grades. Educational Technology Services manages the service, which went live in November 2014 with the service name of bCourses.

The university also has a systemwide agreement with ServiceNow for the use of their products by any of the ten campuses including the medical centers and the Department of Energy National Laboratories. Locally, Campus Shared Services (CSS) uses ServiceNow's service management automation suite for requesting IT service (i.e., service request ticketing system), incident management, and problem management. The service went live in August 2014. Future plans are to utilize this solution to support other information technology service groups on campus and

[1] These tools allow instructors to post announcements, create and send messages, facilitate topical discussions, chat in real time, collaborate with students on the same document, and have virtual lectures or office hours.

across other CSS services (i.e., Human Resources/Academic Personnel Support, Business and Financial Services, and Research Administration).

Summary Conclusion

While the evaluation of cloud service providers generally follows similar practices for the procurement of other services by the campus, internal controls for analyzing requirements, including analysis of costs and risks, and whether service providers satisfy our requirements before acquisition are minimally effective. Due diligence procedures need enhancement to include, for example, analyzing the cost of alternative delivery models and service providers, evaluating the risk that the service provider may not continue to operate, and obtaining assurance the service provider is capable of meeting our security, availability, privacy, and information process requirements. In the absence of these procedures, opportunities to increase cost savings may be lost, service providers may not possess the capabilities to safeguard our data, the campus may engage a service provider where there is substantial doubt about the service provider's ability to continue to operate[2], or service provider's standard terms and conditions may not meet campus requirements.

Once service commences control activities also need strengthening to ensure cloud service providers continue to perform as agreed, meet future campus needs, and provide competitive pricing. There are gaps in the measures of performance and the reporting of those measures to aid managing supplier performance. For example, measures focusing on service usage, user satisfaction, changes to the service (including changes in cost), as well as for ensuring on-going conformance with our security, privacy, availability, and processing integrity needs are currently minimal. The responsibility for regular and formal reporting by cloud service providers is unclear in the contracts we examined, potentially impacting effective contract management. In the absence of these provisions, while cloud service providers may meet our requirements at the time of acquisition or be the best alternative, there is no guarantee they will continue to meet our requirements through the term of the contract or continue to be the best alternative for meeting our needs in the future.

[2] For example, negative trends such as recurring operating losses, working capital deficiencies, or negative cash flow from operating activities, default on a loan, need to seek new sources of financing, or disposition of substantial assets.

SUMMARY OF OBSERVATIONS & MANAGEMENT RESPONSE AND ACTION PLAN

Evaluating Cloud Service Providers

Observation

While the evaluation of cloud service providers generally follows similar practices for the procurement of other services by the campus, internal controls for analyzing requirements, including analysis of costs and risks, and whether service providers satisfy our requirements before acquisition are minimally effective.

There was little to no evidence, in all three contracts examined, of the operation of internal control procedures for evaluating and appraising the cost of different deployment models (cloud vs. non-cloud) and service providers (internal vs. external) to identify the most favorable alternative over the lifecycle (upfront, persist, and termination costs) of the solution. Similarly, analysis was largely not present for evaluating financial stability (liquidity, profitability, credit worthiness, access to capital, etc.), industry (market share – customer base size and growth), and the competitive environment (position and longevity of cloud service providers and their products in the marketplace). Review of the financial stability of cloud service providers did not occur for all three contractual relationships examined. In one contractual relationship, an evaluation of the industry and the competitive environment did occur. By reviewing costs, a lower cost alternative could be identified that could provide a comparable level of service. Also, by reviewing these factors, selection of a cloud service provider that is in poor financial health or is at risk of obsolesce can potentially be avoided.

Further, there was little to no evidence of the operation of internal control procedures, in all three contracts examined, to obtain assurances that cloud service providers are capable of meeting our established security, availability, privacy, and information processing requirements. Examples of such control procedures, depending upon the level of reasonable assurance desired, include

- examining external assessment reports on controls[3];
- inspecting self-assessment[4];
- utilizing questionnaires, reviewing provider policies, or making use of the Federal Risk and Authorization Management Program Security Control Workbook for validating compliance with campus policy; and
- making use of technical demonstrations and site visits to observe cloud service provider controls.

Also, in all three contracts, language was absent from the contract and/or service level agreement specifying time recovery requirements from abnormal working conditions (recovery point and time objectives [RPO and RTO]) and for testing recovery plans and provisions. There was little or no evidence identifying this as a contractual requirement or evidencing the prioritization of

[3] e.g., Service Organization Control Type 2 (SOC 2) report, ISO 27001/2 or Cloud Security Alliance Star Attestation certifications

[4] e.g., cloud service provider internal audit plans and reports or Cloud Security Alliance Star Self-Assessment

this requirement relative to others and ensuing evaluation of this contractual requirement against the contract or service level agreement. Information security, privacy, and regulatory compliance issues associated with unforeseen events resulting in extended downtime or recovery time could potentially be avoided by ensuring the cloud service provider satisfies our requirements before acquisition.

Next, appraisal of potential conflicts between the location of data and United States and international laws and regulations (e.g., export, privacy, and security) were inconsistent. In all three contracts examined, there was little to no evidence of internal control procedures for obtaining assurances that cloud service providers have effective controls in place for restricting the storage of data to specific locations. Guidance offered by the UC Technology Acquisition Support (TAS) group states all rights in and to data remains exclusively the property of the campus and that data must stay within the continental United States. When data is stored in a foreign country, privacy issues and difficulties may surface with returning data upon termination.

Additionally, the contracts or service level agreements were largely silent[5], in all three cases examined, concerning provisions for requesting changes during the term of the contract (e.g., changes in campus policy such as information security policy, legal/regulatory requirements, etc.); any limitations on how much change is allowed; and the process for requesting, approving, and escalating change requests. There was little or no evidence identifying this as a contractual requirement or evidencing the prioritization of this requirement relative to others and ensuing evaluation of this contractual requirement against the contract or service level agreement. While it is inevitable that concessions will have to be made, in the absence of such provisions, it may be difficult to make changes to the contractual relationship during the term of the agreement.

As well, internal controls were not present in two out of the three contracts examined for obtaining assurances the cloud service provider is capable of meeting our support needs and expectations. Examples of internal controls might include periodically reviewing service provider policy and procedures and benchmarking them against industry accept standards (e.g., IT Infrastructure Library), metrics on performance, or interviewing other clients of the service provider. Untimely resolution of requests for support can potentially be reduced or avoided by understanding the cloud service provider's policy, procedures and performance.

Lastly, assurances regarding the cloud service provider's capabilities for meeting our e-discovery needs were missing in all three contracts examined and they were also silent concerning roles and responsibilities related to e-discovery. Difficulties and unforeseen costs may occur with providing data, as needed, during legal or regulatory proceedings.

These observations are present because using cloud computing to deliver services is different from how the campus traditionally has procured and delivered IT services. Additional direction, instruction, and tools to tailor our procurement practices to cloud computing contracts would be helpful to aid stakeholders who do not routinely enter into contracts for cloud service to know what to consider and how to go about efficiently and effectively selecting a cloud service that best meets their needs while minimizing risks. How this might look would be to provide direction, instructions, and tools for evaluating cloud service providers, such as

---

[5] The terms and conditions for the Google agreement give us the right to decline changes Google makes that materially negatively impact the campus, however, provisions for changes at our request is not present.

- defining what requirements should be considered,
- prioritizing requirements, based upon established evaluation criteria, for scoring the requirements on importance and how well the solution meets requirements,
- distinguishing where formal evaluation is mandatory[6],
- evaluating and appraising the service delivery costs of different deployment models (cloud vs. non-cloud) and service providers,
- selecting evaluation methods and alternatives, and
- obtaining approval on the solution that represents the best fit.

In addition, cloud tailored templates for requests for information or proposals, service level agreements and contracts represent an opportunity to streamline the process, increase understandability of the full set of requirements and work flow, and promote consistency in the performance of controls. This is especially true in the case of information security since our campus requirements (e.g., Minimum Security Standards for Electronic Information) go beyond those contemplated by the University of California Data Security and Privacy Appendix DS.

Management Response and Action Plan

Cloud Sourcing Strategy

Management will articulate a high level cloud sourcing strategy that addresses approaches to managing cloud specific risks in a balanced risk manner by October 1, 2015.

Guidelines

Management will continue to engage with the UC Cloud Services Workgroup, charged with sourcing cloud services contracts for all campuses to use, to iteratively develop resources and guidance to aid in managing risks associated with the acquisition and use of cloud services. A near term deliverable has been implemented, deployment guides for seven UC Cloud contracts perceived to have the widest adoption across the UC System.

Templates Evidencing Cloud Service Owners' Due Diligence

An EDUCAUSE Center for Analysis and Research working group developed a total cost of ownership (TCO) tool for effectively identifying and comparing TCO for both cloud-based and on premises fulfillment of IT services. The tool is available on the EDUCAUSE workgroup's website. Management will shortly make this framework available in a location accessible to the campus.

Management will develop a cloud services risk assessment and mitigation form that: 1) articulates key risks and considerations for cloud service engagements; 2) provides a space to articulate how these general risks apply to a specific engagement under consideration; 3) provides a space to articulate specific risk mitigation plans; and 4) includes a signature block for acceptance by the business owner of the risks and mitigation plans. The planned implementation date is October 1 2015.

---

[6] e.g., cost, security, availability, privacy, compliance, control, and legal/contractual issues

Confirming and Reporting on Cloud Service Provider Performance

Observation

Control activities need strengthening to ensure on an ongoing basis that providers perform as agreed, continue to meet future campus needs, and provide competitive pricing. Measures specified in the contract and/or service level agreement mainly focus on uptime and support (e.g., hours of support and target response times). Other examples of measures or activities for ongoing monitoring of performance include

- service usage counts,
- user experience rating,
- changes to the service,
- financial details[7],
- results of third party assessments,
- results of service provider internal assessments,
- availability measurements,
- capacity indicators,
- issues and action items,
- results of reviews of the contracts and service agreement to ensure they are up-to-date, and
- industry and market analysis comparing current service provider with alternate supplier service offerings and value for money.

Furthermore, at present, the contract language obligating the provider to provide regular reporting on uptime and level of support is missing. Also, internal reporting by campus personnel to management, to aid in performance management, is currently ad hoc, reactionary and discretionary rather than regular and formalized.

While cloud service providers may meet our requirements at the time of acquisition, there is no guarantee they will continue to meet our requirements, for example, security, availability, privacy, and information processing through the term of the contract. In addition, we may miss future cost saving opportunities or may not timely identify trends that suggest that users are no longer satisfied with the quality of the service delivered or value for the money.

These conditions come about because, for instance, awareness about these other performance measures has not yet fully materialized. Direction, instructions, and/or tools detailing what should be considered and a process for prioritizing these requirements would likely increase understanding and help in implementing controls for developing, evaluating, and negotiating contracts and service level agreements. Furthermore, awareness and understanding has not yet fully materialized concerning the limitations and potential effects when relying upon a reactionary and discretionary approach to performance monitoring and reporting. A discretionary and reactionary approach is likely inconsistent, incomplete, and ill-timed in terms of yielding information necessary for effective performance management. Direction and instruction distinguishing when formal monitoring and reporting is necessary would likely be helpful to ensure that, at a minimum, monitoring and reporting is occurring for significant cloud

[7] e.g., current cost or anticipated cost increases

service providers. Also, direction and instruction would likely be helpful to unit-level management in understanding what is expected of them and what post implementation roles and responsibilities look like, for example, defining objectives and responsibility for monitoring and reporting, required activities, frequency, and tools for evaluating and reporting (e.g., reporting templates).

Management Response and Action Plan

Parts of the management response and action plan from the first observation are also responsive to this observation, for instance, the responses under the headings of Cloud Sourcing Strategy and Guidelines. In addition, under the heading labeled Templates Evidencing Cloud Service Owners' Due Diligence the cloud services risk assessment and mitigation form listing risk factors and risk mitigation plans should take into consideration risks over the lifecycle of the relationship with a cloud service provider.