UCIrvine | Internal Audit Services

Cloud Computing

Internal Audit Report No. I2019-105

September 24, 2019

Prepared By
Larry Wasan, Principal IT Auditor
Reviewed and Approved By
Mike Bathke, Director

UNIVERSITY OF CALIFORNIA, IRVINE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

INTERNAL AUDIT SERVICES
IRVINE, CALIFORNIA 92697-3625

September 24, 2019

SNEHAL BHATT
CHIEF PROCUREMENT OFFICER AND DIRECTOR
PROCUREMENT SERVICES

KIAN COLESTOCK
INTERIM CHIEF INFORMATION OFFICER
OFFICE OF INFORMATION TECHNOLOGY

Re: Cloud Computing
No. I2019-105

Internal Audit Services has completed the review of UC Irvine Cloud Computing.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting our review. If you have any questions or require additional assistance, please do not hesitate to contact me.

Mike Bathke
Director
UC Irvine Internal Audit Services

Attachment

C: Audit Committee
Josh Drummond – Chief Information Security Officer, OIT

I. MANAGEMENT SUMMARY

In accordance with the fiscal year (FY) 2018-2019 audit plan, Internal Audit Services (IAS) reviewed the processes in place for the University's procurement of third-party cloud services, including policies and strategies, vetting of contracts, and ongoing monitoring and management of cloud services to ensure the protection of University data. While some internal control activities were noted by IAS, the review identified opportunities for improvement to minimize business risks, strengthen information security controls, and ensure compliance with security policies and regulations. The following observations were noted.

Cloud Computing Governance – Management does not have a formalized cloud computing strategy. There are no documented cloud computing policies and procedures, and cloud management roles and responsibilities were not clearly assigned. This observation is discussed in section V.1.

Vetting of Cloud Contracts – Although management stated that they have a process for vetting cloud computing purchases, the process is not documented, is ad-hoc, and is not consistently performed. This observation is discussed in section V.2.

Cloud Computing Inventory – Management confirmed that there is no inventory of cloud computing services and there is no classification for cloud computing services in the Kuali Financial System (KFS), the University's comprehensive accounting and procurement application. This observation is discussed in section V.3.

II. BACKGROUND

Cloud computing refers to computer software, hardware, and network infrastructure that is provided and managed by a vendor and accessed by users via the internet. Cloud computing services can be in various forms, which includes Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). This review is focused on SaaS, which includes not only the software, but also the servers in which the software resides and the network system that allows access via the internet. University data may also

reside on the vendor's servers, which is one of the major concerns with cloud computing services, especially as it relates to restricted or sensitive data.
With SaaS, the vendor is responsible for virtually all technical aspects of the cloud service, including application and systems maintenance, upgrades, end-user support, cybersecurity, and disaster recovery/business continuity planning and testing. For these reasons, cloud computing is typically much more cost-effective than on-premise applications, and organizations of all sizes, including UC Irvine, are transitioning or have transitioned to cloud computing as a model for enterprise level as well as for department/unit level computing resources.

Procurement of cloud services by UC Irvine departments/units can be made through Procurement Services via Purchase Orders (PO). Procurement of cloud services can also be made with a PALCard, which can be used for purchases of $5,000 or less, and therefore is below the approval threshold of Procurement Services management.

III. PURPOSE, SCOPE AND OBJECTIVES

The purpose of the audit was to review UC Irvine's cloud computing governance, which includes strategies, policies and procedures, and management roles and responsibilities; vetting of cloud computing contracts; and the ongoing management of current cloud services. The scope was limited to SaaS cloud computing contracts within the University Campus and did not include cloud computing services at the Medical Center nor UC-systemwide cloud contracts.
The following audit objectives were included in the review.

1. Verify the existence of a documented cloud computing strategy and review for alignment with UC Irvine's business goals and objectives, including the UC's Electronic Information Security Policy (IS-3).

2. Review cloud computing policies and procedures and verify that it includes key information to protect the Campus from various cloud computing risks. Verify compliance with such policies, procedures, and guidelines.

3. Verify that management responsibilities for cloud computing services are assigned, formally documented, and approved. Verify that management is aware of their assigned responsibilities.

4. Verify that cloud computing contracts are adequately vetted and approved.

5. Verify the existence and adequacy of a cloud computing inventory system.

IV. CONCLUSION

Some internal controls are in place to protect the University's interests, including protections for restricted data; however, opportunities for improvement and concerns were noted regarding cloud computing strategy, policies and procedures, assignment of roles and responsibilities, vetting of contracts, and cloud computing inventory and monitoring.

Observation details were discussed with management who formulated action plans to address the issues. These details are presented below.

V. OBSERVATIONS AND MANAGEMENT ACTION PLANS

1. Cloud Computing Governance

A. Cloud Computing Strategy

Observation

Interviews with management from the Office of Information Technology (OIT) and Procurement Services confirmed that there is no formalized and documented cloud computing strategy. Consequently, IAS was unable to determine whether or not cloud computing activities and strategies are in alignment with business objectives. With the organizational trend towards cloud computing services and away from on-premise applications, it is important to have a strategy in place for how cloud computing contracts and services should be managed by the University. The lack of a

formalized and documented cloud computing strategy poses the risk of management activities being performed that are inefficient, ineffective, and/or inconsistent with business goals and objectives.

Additionally, as part of overall IT governance and cloud strategy, according to Section 5.1 of the UC's IS-3 policy, "Locations must establish and implement an Information Security Management Program (ISMP)" which includes the following ISMP elements:

5.2.1 Information Security Risk Governance
5.2.2 Unit security planning, execution and review
5.2.3 General security and awareness training
5.2.4 Reporting on risk and the state of information security
5.2.5 Operationalizing information security

Management Action Plan

By May 31, 2020, OIT will establish an Information Security Management Program (ISMP) aligned to IS-3 and develop a supporting implementation plan.

By July 31, 2020, OIT will develop a cloud computing strategy and framework.

B. Policies and Procedures

Observation

Interviews with management from OIT and Procurement Services confirmed that there is no formalized cloud computing policies and procedures document. Although a document containing cloud computing guidelines was available online, it is not an official policy document, and management stated that the guideline was optional. A detailed and formalized cloud computing policies and procedures document provides management and staff with guidelines and requirements that must be adhered to, creates process consistency, and helps prevent errors, omissions, and misuse of resources.

Management Action Plan

By May 31, 2020, OIT will formally specify cloud computing policies, standards, and procedure requirements aligned to IS-3.

C. Management Roles and Responsibilities

Observation

With a lack of formalized policies, procedures, and strategies also comes a lack of a clear assignment of roles and responsibilities for the management of cloud computing contracts and services, specifically in the areas of data ownership, security, and compliance. Without a clear assignment of roles and responsibilities, critical processes, such as identification of assets, risk assessments, vetting of contracts, and monitoring of cloud services, may be omitted or inconsistently performed, and it is difficult to assign accountability for any issues that may arise.

Management Action Plan

By May 31, 2020, OIT will partner with Procurement Services to develop and assign roles and responsibilities for the management of cloud computing contracts and services.

2. Vetting of Cloud Computing Contracts

Background

Initial vetting of cloud contracts is typically performed by Procurement Services, and if it is identified that restricted or sensitive data will be used or stored in the cloud, Procurement Services will refer the matter to OIT for additional vetting.

It is extremely important that the University thoroughly vets cloud computing contracts and services to ensure that terms and conditions protect the

University's interests and effective controls are in place to maintain the confidentiality, integrity, and availability of University data.

Observation

Vetting of cloud computing contracts procured with PO's is performed on an ad-hoc basis, and according to management, the process is not documented. Consequently, IAS was not able to review the effectiveness of management's vetting process.
In addition, although some cloud purchases made with PALCards may be brought to the attention of Procurement Services for vetting, it is not required by policy and appears to be inconsistently performed. Furthermore, according to OIT management, they do not have visibility to cloud purchases made with PALCards. Consequently, they are also unable to vet the contracts prior to purchases being finalized.

Management Action Plan

By May 31, 2020, OIT will partner with Procurement Services to develop a formal cloud computing contract vetting process.

By July 31, 2020, OIT and Procurement Services will develop and deliver communication and training for purchasers (including PAL Card users) on the new cloud computing contract vetting process.

3. Cloud Computing Inventory and Monitoring

Observation

Management did not have a complete and up-to-date cloud computing services inventory, and although there is a general classification for software PO's in KFS, there is no classification specifically for cloud computing services. Therefore, Procurement management could not readily identify PO's for cloud computing services.
Although Procurement Services was able to perform a search and identify some cloud computing services purchased via PALCards, the search could only be conducted for known cloud computing services, and cloud computing

services unknown to management would not have been identified in the search.
Due to the lack of a complete cloud services inventory, IAS was unable to choose a representative sample of cloud contracts for review to verify appropriate terms and conditions and ensure that University interests are protected.
In addition, according to the UC IS-3 policy, Section 6.1, risk management minimum requirements includes, among others, identifying assets, monitoring risks on an ongoing basis, and monitoring security and compensating controls for effectiveness. Section 6.1.1 also states that "Risk Assessments must include . . . cloud and supplier services for institutional information classified at Protection Level 2 or higher."

Not having a cloud computing inventory system or a category for cloud computing services in KFS does not allow for the identification and classification of assets, risk assessments, and regular monitoring of controls for effectiveness as required by the UC IS-3 policy.

Management Action Plan

By July 31, 2020, Procurement Services will develop and maintain an inventory system or category for cloud computing services.