Third Party Provider – Google Inc.

November 2014 **FY15 - #10**

Submitted to:

Karen A. Williams, Interim Vice President, Information Technology and Chief Information Officer
Derek A. Masseth, Deputy Chief Information Officer and Chief Technology Officer

Copies to:
Institutional Internal Audit Review Board
Audit Committee, Arizona Board of Regents
Andrew C. Comrie, Senior Vice President for Academic Affairs and Provost
Gregg Goldman, Senior Vice President for Business Affairs and Chief Financial Officer
Laura Todd Johnson, Vice President, Legal Affairs and General Counsel
Jon Dudas, Senior Associate to the President and Secretary of the University
Duc D. Ma, Interim Associate Vice President, Financial Services Office

Issued by: Sara J. Click, CPA, Chief Auditor
Internal Audit Department

Summary

Our audit of the University's agreement with third party provider, Google, Inc. ("Google") was included in the approved Fiscal Year ("FY") 2015 Audit Plan. Effective management of Information Technology ("IT") supports the Never Settle strategic plan's "Synergy" strategic priority. The Synergy priority includes actions to optimize our physical resources and virtual reach in expanding and aligning IT capacity. This is our first audit of the agreement with Google.

Background: Google is a global technology company that provides productivity tools and services in an integrated environment allowing for efficient communication and collaboration. Google's business focus is broad and includes online search services, cloud services, advertising, operating systems, platforms, enterprise services, and hardware products. Google is considered the pioneer of online advertising; reports estimate that a large portion of Google's revenue is generated from online advertising.

In 2009, the University of Arizona signed a no-cost agreement with Google in response to requirements to provide a more reliable, robust email service for students. Arizona State University and Northern Arizona University also have agreements with Google.

University Information Technology Services ("UITS") is responsible for management of the vendor, the agreement, and the integration\administration of Google products and services. Student Affairs Enrollment Management – Academic Initiatives and Student Success ("SAEM-AISS") is considered the business owner and is responsible for representing the requirements of the students.

Although email is the primary purpose for the agreement with Google, the University offers the full suite of Google Apps for Education ("GAE") products to students, faculty, and staff. IT support efforts are focused mainly on Google Gmail as it is considered the official communication method for informing students of University business. The University refers to the Gmail product within GAE as CatMail; all enrolled students, faculty, and staff are eligible for an account. The CatMail account provides access to the Google products and services; the accounts are never deactivated regardless of enrollment or employment status. For faculty and staff, the Gmail product is enabled. However, they cannot send or receive email from the Gmail interface within GAE.

The application suite offered by Google, GAE, includes a wide array of applications in addition to email. The products include productivity and social media applications and unlimited cloud storage. Although the University maintains a separate Microsoft Exchange email system for employees and offers site licenses for Microsoft Office and

Box, faculty and staff can choose to use Google products for University business and store files with Google. Since Google products and services enable collaboration and the ability to use office productivity tools such as word processing in an integrated environment, they are popular amongst University students, faculty, and staff.

Google makes changes and additions to their products and services often. When the University signed the agreement with Google in 2009, the data storage limit was one gigabyte per user. Currently, the storage is unlimited and is free of charge via the Google Drive service. The data is stored in Google data centers located globally. Users have no control over the geographic location of the data. Google representatives contacted during fieldwork stated that the GAE data storage environments are more controlled than the consumer environments due to increased regulatory requirements.

Google has achieved industry standard certifications from the International Organization for Standardization ("ISO")[1] and the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements ("SSAE")[2]. The certifications are attained yearly and imply a high level of security and operational effectiveness. As a result, the Chief Information Officer's ("CIO") Office believes there is minimal risk related to general information security controls at Google facilities. Risk regarding Google product use is related to the user and awareness of University information security policies and the University's GAE administration practices. Current University policy prohibits confidential and regulated data from being processed, transmitted or stored with Google Drive and CatMail\GAE (unless properly encrypted).

Google Drive provides the capability for the user to easily share files and folders publically and with others external to the University. Currently, 4,000 of the 9,000 employee accounts have opted to share information publically. Google provides an Administrator Console with GAE to enable organizations to establish controls regarding sharing data and to administer the products used by students and employees. Since Google is primarily viewed by the University as a student email service, data storage is not actively monitored and administration efforts are minimal.

Employee Microsoft Exchange email accounts are deactivated when employees leave the University. However, the employee Google accounts remain active. Information provided during fieldwork indicated that there were over 160,000 Google accounts; approximately 9,000 of the accounts were employee accounts. Since the Google accounts are unlimited and free, there is no monetary reason to manage them other

[1] International Organization for Standardization ("ISO") is an international standards organization. ISO 27001 is an information security standard which outlines controls and processes that are required to achieve ISO 27001 certification.

[2] SSAE 16 Service Organization Controls 2 and 3 ("SOC") includes trust service principles and criteria for controls related to availability and security of information.

than for compliance with policies such as information security or email. Google offers the unlimited accounts as the majority of their revenue is derived from online advertising. By offering unlimited licenses, Google increases the user base exponentially and in turn can increase advertising revenue.

In the past year, concerns have been raised by educational users, regarding Google's practices of scanning email content and mining data to support targeted advertising. As a result, Google has removed ad scanning for GAE. However, Google continues to scan and serve ads to educational users who use the non-core products and services. The non-core products include Google Plus, YouTube for Schools, Google Moderator, Apps Marketplace, Chrome, Translate, Google Apps Script, Custom Search, Maps, Voice, Blogger, Scholar, Books, Code, and Picasa Web Albums.

Audit Objective: Our audit objective was to perform a vendor management review to ensure that service level expectations such as incident response, performance and availability are addressed in the agreement along with provisions for security controls, data confidentiality, change management, and disaster recovery. We also reviewed the security provided by Google Inc. for University and student data to determine if University policy, legal, and regulatory requirements were met.

Scope: The scope of the audit is a review of the processes and controls in place during the audit period (September – November 2014) for the Google agreement and the access to products and services provided to students and employees.

Methodology: The audit objectives were accomplished by performing a review of general controls based on the ISACA Cloud Service Provider audit work plan and the Institute of Internal Auditors ("IIA") guidance for Third Party Risk Management.

- Interviewing University staff and management within the CIO's Office who have responsibility for IT management, information security management, IT vendor management and staff and management within Student Affairs who have responsibility for student IT experiences:
    - CIO's Office
        - Former CIO
        - Former Deputy CIO
        - Director of Cloud Computing (Now, Deputy CIO and Chief Technology Officer)
        - Director of Business Services
        - Information Security Officer
    - UITS
        - Principal Systems Administrator

  - Student Affairs and Enrollment Management
    - Senior Vice President
    - Associate Vice President

- Interviewing the Google Higher Education Business Development/Sales Representative assigned to the University.

- Reviewing existing University policies and standards related to information technology operations and information security.

- Reviewing regulatory requirements such as the Family Educational Rights and Privacy Act (“FERPA”), Children’s Online Privacy and Protection Act (“COPPA”).

- Reviewing and comparing the original Google agreement (2009) with the newer online agreement (2012).

- Researching the risks associated with Google’s data mining practices.

Conclusion: UITS has effective practices in place to manage the financial aspects of vendor agreements. However the controls to ensure that vendor performance and risk are managed on a consistent basis for all agreements regardless of cost require improvement. Since vendor management is largely focused on financial aspects, the risks and impacts for a no-cost agreement such as Google can easily be overlooked, for example, the changes in capacity for Google Drive and other Google products. A risk assessment regarding storing data with Google and faculty/staff use of GAE has not been completed since 2012.

Although Google’s service level performance is not actively monitored, UITS views the services as stable and secure and, therefore, low risk from an IT operations perspective. CatMail is considered the most critical application of the GAE suite in support of the University’s mission. UITS indicated that CatMail outages have been minimal since 2009.

Although Google obtains appropriate certification regarding information security, UITS does not consistently request and maintain the certifications as part of the vendor management process. We found that the risks associated with the location of the Google data centers and the choices students and employees can make when storing data have not been assessed by the University. Google Drive provides an option to share data publically on the web. Capability exists to disable this option for all users and should be investigated as the controls in place at the Google data centers could easily be negated. Additionally, the Information Security Data Classification and Handling Standard (IS-2321) states that confidential and regulated data cannot be stored with Google. While it is not possible to control the actions of individuals and where they store data, it is possible to provide guidance related to policy and make use of the administrator capabilities to manage risk.

Since Google accounts are free and unlimited, usage is not monitored. Therefore, accounts are not deactivated for students or employees as they would be if there were a cost per user. We found that the risks and impacts associated with offering lifetime accounts given the current Google product offerings that include social media applications, and a web browser had not been assessed by the University. Discussions with the CIO, UITS, and SAEM-AISS indicated that there is no process in place to ensure that risk and impacts are assessed related to the use of GAE or before implementing new or modified products. UITS reviews the change if the impact is related to cost, for example, changes requiring additional hardware. An integrated governance process for mission critical or enterprise applications/services such as CatMail and GAE would allow the business sponsor and IT to assist in assessing risk before implementation to students and employees.

Google has become much more than a student email service; it is a widely used enterprise cloud service used by University students and employees. Recent news regarding Google indicates that there could be future legal risk related to Google's scanning practices and targeted advertising in the education sector. Since the University sponsor's the service and makes decisions regarding the products and services offered, appropriate guidance should be provided, and acceptance of risk and University policy should be obtained by all users during provisioning.

According to the Institute of Internal Auditors International Professional Practices Framework, an organization is expected to establish and maintain effective risk management and control processes. These control processes are expected to ensure, among other things, that:

- The organization's strategic objectives are achieved;
- Financial and operational information is reliable and possesses integrity;
- Operations are performed efficiently and achieve established objectives;
- Assets are safeguarded; and
- Actions and decisions of the organization are in compliance with laws, regulations, and contracts.

Our assessment of these control objectives as they relate to the agreement with Google is presented on the following page.

General Control Objectives	Control Environment	Audit Result	
		No.	Page
Organizational Strategic Objectives are Achieved			
• Google products and services meet the requirements for student email communication.	Reasonable to Strong Controls in Place		
Reliability and Integrity of Financial and Operational Information	Not Applicable		
Effectiveness and Efficiency of Operations			
• The Google agreement contains provisions for incident management, performance\availability, security controls, data confidentiality, change management, and disaster recovery.	Reasonable to Strong Controls in Place		
• Processes to manage risk related to changes and additions to Google products and services are in place and functioning effectively.	Opportunity for Improvement	1	7
• Documented processes to manage vendor service levels are in place and functioning effectively.	Opportunity for Improvement	2	10
Safeguarding of Assets			
• The security provided by Google meets University policy, legal, and regulatory requirements.	Opportunity for Improvement	1	7
Compliance with Laws and Regulations			
• The Google agreement sufficiently meets requirements for FERPA and other regulated data.	Reasonable to Strong Controls in Place		
• Controls exist to ensure Google product usage is in compliance with University policy, and legal, regulatory requirements.	Opportunity for Improvement	1	7

We appreciate the assistance of UA Staff during the audit.

/s/

Rosemary R. Casteel, CISA
Auditor-In-Charge
(520) 626-4235
casteelr@email.arizona.edu

/s/

Sara J. Click, CPA
Chief Auditor
(520) 626-4155
clicks@email.arizona.edu

Audit Results, Recommendations and Responses

1. Controls for management and administration of Google products and services are not sufficient to assess the risks associated with data security and employee use.

Condition:
Google products are not consistently administered and managed. Accounts are never deactivated, and controls for data security are not reviewed. Employee use of the products and services has not been assessed to ensure that risks are known and managed.

Criteria:
ISACA's Control Objectives for Information Technology ("COBIT") indicates that the following should be in place to ensure effective management of information technology, risk and ensure that informed decisions are made:

- IT organizations, information security, and University management operate in a defined integrated governance framework and monitoring process.
- Processes that require a review of new and modified technologies and vendors to validate adherence to University policy and other relevant regulatory and legal requirements.

Causes:
- Google is a no-cost agreement.
- A process for reviewing changes to products/services is not in place. Therefore, sufficient risk and impact assessment of Google products and services has not occurred since 2009.

Effects:
- Information security risks associated with storing and sharing confidential and regulated data with Google.
- Risk associated with providing students and employees with lifetime accounts sponsored by the University.
- Risk associated with offering Google products without assessing impacts such as social media products.
- Cost efficiencies related to Microsoft Office licenses and other products such as cloud storage subscriptions that may not be needed if Google offerings meet University requirements.

Recommendations:
We recommend UITS along with appropriate University management take the following actions:

General Oversight and Risk Management:

- Implement a process for change management for Google products and services that includes the appropriate University management for decisions regarding employee and student usage. The process should include an impact and risk assessment for products and services.
- Review the Google products available for use and assess the risk associated with each product and the two user communities (students and employees).
- Determine if accounts should be deactivated when enrollment or employment ends.
- Review Google Drive data security controls such as public sharing and assess the risk of student and employee data stored with Google.
- Assess the cost efficiencies of using Google products and services over Microsoft Office products and other services such as Box and DropBox and inform campus management of results.

Google Product Management and Administration:

- Provide specific guidance regarding University policy for students and employees and storing confidential and regulated data with Google.
- Require acceptance of applicable University policies before granting access to Google products and services.
- Update the web pages that provide the access to Google products and services to reflect current products and services.
- Review the Google Admin console and determine appropriate levels of administration and management for accounts and data storage.

Management Response:
UITS management will undertake the following actions:

- Identify a service owner for the GAE portfolio, this role will be responsible for:
  - Regular review of new service offerings
  - Engage appropriate stakeholders in determining the impacts of changes to the portfolio
  - Review and update the web pages describing the service(s) available
  - Require acceptance of applicable University policies prior to granting access, including data classification guidance
  - Review the Google admin console and assess access to Google products and services

- Assess the risks associated with delivering each of the services in the GAE portfolio, led by the GAE Service Owner

There are commercially available products designed to review data security controls and the likelihood of private or regulated data in the Google Drive environment. UITS management will assess available tools and propose funding support for the best fit product.

It is the opinion of the Office of the CIO that, in light of the diversity of the community, the University community can and should make use of a diverse tool set, including but not limited to Google Apps for Education, Box, Office 365, Dropbox and others. The appropriateness of a particular solution depends strongly on the capabilities of the collaborators, sensitivity of data, and functionality required.

Specific guidance regarding the storing of confidential and\or regulated data is published online at:

http://security.arizona.edu/data-classification-and-handling-standard

This guidance will be referenced in the new website regarding the availability of the GAE portfolio.

Target Implementation Date: July 31, 2016.

2. UITS vendor management controls related to risk and performance monitoring require strengthening.

Condition:
Vendor performance monitoring and risk management is decentralized within UITS. Service levels are not tracked and managed with formal reporting and metrics. Risk and impact assessments are not required for changes to products, services, and the agreements.

Criteria:
ISACA's Control Objectives for Information Technology ("COBIT") indicates that the following should be in place to ensure effective management of information technology, risk, and to ensure that informed decisions are made:

- Monitor service levels, report on achievements and identify trends to aid in performance management.
- Conduct periodic reviews of agreements and revise when needed.
- Manage, maintain, and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal/regulatory requirements.
- Continually identify, assess, and reduce IT-related risk within levels of tolerance set by enterprise executive management.

Cause:
Within UITS, vendor management is predominately focused on financial management and budget monitoring rather than vendor performance and risk management. Vendor management is provided by the UITS Business Office, whose primary responsibility is to provide financial management services to UITS and the CIO's office.

Effect:
Lack of formal risk and performance management can lead to degraded service and noncompliance with University policy and other regulatory/legal requirements.

Recommendations:
The CIO should ensure that sufficient controls and processes are in place to ensure the following:

- Vendors and contracts are assessed periodically to ensure that contract terms are valid.
- Risk related to contracts is reviewed and managed regardless of cost.
- Vendor certifications regarding information security or other operational certifications are requested and managed by UITS.
- Service and performance levels that are specifically stated in the agreements are measured and reported by the units responsible for managing the vendor.
- Impacts to vendor agreements resulting from changes to internal policy or regulatory/legal requirements are assessed to determine appropriate action, for example, General Counsel review.

Management Response:
UITS management will:

- Work to insure that all contracts, regardless of associated costs, are included in an annual review process.
- The annual review process will collect and maintain relevant information security and operational certifications.
- The annual review process will also consider changes to internal policy or regulatory\legal requirements to determine appropriate action to take.

Target Implementation Date: July 31, 2016.