INTERNAL AUDIT
IAS
ADVISORY SERVICES

Internal Audit Report

IT Cloud Computing

Report No. SC-16-01
February 2016

David Lane
Auditor-in-Charge

Approved
Barry Long, Director
Audit & Management Advisory Services

UC SANTA CRUZ

This page intentionally left blank

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2

II. INTRODUCTION

Purpose 3

Background 3

Scope 4

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A. IT Cloud Services Business Contracting 6

B. Cloud Governance and Guidance 11

C. Assurances of IT Cloud Service Provider Maintained Controls 13

APPENDICES

A. NIST Special Publication 800-145 – The NIST Definition of Cloud 15

B. UC Data Security and Privacy (Rev. 10/27/14) "Appendix DS" 18

C. ITS Website - Amazon Web Services 19

D. UC Irvine – IT Cloud Service Provider Ratings 23

E. Google Service Organization Control (SOC) 3 Report 24

I. EXECUTIVE SUMMARY

Audit & Management Advisory Services (AMAS) has completed an audit of the adequacy of controls over the contracting with third-party cloud computing service providers, the effectiveness of IT cloud computing governance, and the level of assurances provided over information security controls of data stored in the cloud.

Overall, IT cloud computing controls were generally effective in assuring data was protected and data integrity was maintained both within campus enterprise systems and addressed within vendor contracts administered by ITS and Procurement Services. In addition, University contracts including Amazon Web Services provided a more controlled way for users to engage in IT cloud computing services and in the case of Google, fundamental core applications used at UCSC.

However, in the absence of any overarching systemwide or campus IT cloud computing use policy and formalized contracting process protocols, ITS and Procurement Services have created ad-hoc processes to address the unique IT cloud contracting needs. Opportunities were identified for strengthening, standardizing, and improving some IT cloud contracting processes, addressing ways to ensure the reliability of data classification levels self-reported by users, and seeking third-party assurance, such as a SOC 2/3 report on information security controls in place for IT cloud service providers when entering into an agreement.

In addition, the proliferation of IT cloud service providers and the ability of campus users to use cloud services without a campus agreement places even more emphasis on the need for education and guidance for users to ensure that the use of cloud services does not place University data or systems at risk. The campus did not have a way to readily identify its cloud providers that would help in maintaining an ongoing monitoring activity or information that could help faculty and staff in the selection of preferred cloud providers not already contracted with by systemwide or the campus and allow the campus a way to review and evaluate these providers. In acknowledgment of this condition, a project that aims to provide faculty with detailed information about risks and benefits of instructional cloud computing services, as well as local instructional streaming services has begun.

A. IT Cloud Services Business Contracting
Opportunities were identified for strengthening IT cloud service contracts by implementing steps to improve assurances on client reported data classification levels and by considering business criticality when establishing agreement requirements.

B. Cloud Governance and Guidance
IT cloud services governance and supplier management is immature, and lacks an overriding systemwide or campus policy and guidance for acquiring and or administering new IT cloud computing services. The campus does not have a means to provide advice or guidance about cloud service providers to end users who choose to use instructional or administrative cloud computing services.

C. Assurances of IT Cloud Service Provider Maintained Controls
Assurances of the existence and adequacy of security controls maintained by IT cloud service providers was not always obtained prior to releasing data or receiving IT cloud services.

Management agreed to all recommended corrective actions. Observations and related management corrective actions are described in greater detail in section III of this report.

II. INTRODUCTION

Purpose

The purpose of the review was to assess the effectiveness of campus governance and contracting with third party IT cloud service providers, and mechanisms in place to assure the adequacy of information security controls over University data transmitted and stored in the cloud.

Background

The history of cloud computing goes all the way back into the 1960's when it was envisioned that everyone on the globe would be interconnected and accessing programs and data at any site, from anywhere. Since the Internet only started to offer significant bandwidth in the nineties, cloud computing for the masses has been delayed. One of the first milestones in cloud computing history was the arrival of Salesforce.com in 1999, which paved the way for software firms to deliver applications over the Internet.

In 2002, Amazon Web Service (AWS) provided a suite of cloud-based services including storage, computation and even human intelligence through the Amazon Mechanical Turk. Then in 2006, Amazon launched its Elastic Compute cloud (EC2) as a commercial web service allowing small companies and individuals to rent computers on which to run their own applications. Amazon EC2 was said to be the first widely accessible cloud computing infrastructure service.

At UCSC, cloud computing is used in approximately 29 software as a service (SaaS) campus enterprise-like systems, including the procurement system (CruzBuy), the time reporting system (CruzPay), human resources recruitment management system (RMS), eCommons, and many other systems. Enterprise-like cloud systems are established with either local or systemwide business contracts in place with the cloud providers and are typically supported at the local level by the Information Technology Services (ITS) organization. The campus also participates in a systemwide contract with Google Apps for Google cloud services, including Mail, Calendar, Drive, Groups, Sites, Classroom Hangouts, and Vault. The UCSC web page related to Google Apps advises users to not upload restricted data unless required, and then only after it has been encrypted.

Cloud computing is used by faculty to provide information to their students, via SaaS sites without campus agreements including written materials, audio and video, and streaming files. Instructional cloud computing is generally managed by faculty with minimal governance or support.

A large number of staff and faculty use cloud services for file sharing and University business and classroom related purposes, which is also largely self-managed. These services may be offered free through a "click-through" agreement and/or they may also require payment by students or others. In either case, these agreements are nearly always non-negotiable and terms, conditions, and related controls in place are established and controlled by the service provider. Self-managed services of this kind may increase the University's risk because it is unclear what general security provisions are in place to prevent the loss of service, data and exclusivity of intellectual rights.

ITS assists campus users with infrastructure as a service (IaaS) cloud computing through a University contract with AWS, and has posted a Decision Tree and Cloud Metrics diagram on their website to assist users with understanding security requirements for using public cloud computing. AWS is considered appropriate for certain types of confidential data, but restricted data should never be stored in the cloud. Two public cloud

options using AWS include Self Service Cloud Computing, allowing users to engage with cloud service providers themselves, or Managed Cloud Services, where ITS can help users set up and manage IAAS cloud services.

On-Premise cloud computing is a third service available to campus users that are similar to AWS and is managed by ITS and run on pilot software from Joyent SmartDataCenter. However unlike AWS, this service is based on servers and storage physically located in the Data Center at UCSC. This service is not architected for high availability, or to house confidential or restricted data, and is best suited to group or department websites, self-managed developer sandboxes, and non-critical applications with relatively low processing, storage, security and resiliency requirements.

Scope

The National Institute of Standards and Technology (NIST) Special Publication 800-145 provides a definition of cloud computing that was used to determine the scope of our review. (Refer to Appendix A)

This review included inquiry and testing in the following areas:

IT Cloud Governance:
Reviewed governance structure in place (authorization, assessment, roles and responsibilities, etc.). Searched for and reviewed appropriate policies/procedures/guidelines established and implemented. Reviewed process for developing appropriate agreements for cloud service providers. Reviewed process to monitor for the use of cloud services.

Use of Cloud Services:
Interviewed selected ITS, Procurement and other staff to obtain a list of UCSC enterprise-like systems that use cloud technology. Interviewed infrastructure security to determine if and how they identify or monitor cloud usage.

Local IT Cloud Contracts:
Identified cloud services in use supported by campus agreements. Reviewed process whereby cloud agreements are drafted and executed by business contracts. Examined roles and responsibilities of procurement/business contracts, clients and ITS. Selected a sample of cloud computing agreements for review to ensure they contained appropriate terms and conditions, such as UC Data Security and Privacy (hereinafter, “Appendix DS”).

Systemwide IT Cloud Contracts:
Reviewed contract templates, systemwide agreements and procurement processes. Examined if and how UCSC uses templates. Examined if system-wide terms and conditions and Appendix DS addressed all cloud risks. Examined if guidance exists for suppliers who will not agree to Appendix DS or to standard terms and conditions. Interviewed UCOP staff from Procurement and Legal Counsel.

Cloud Security Controls at Local Level:
Interviewed IT Security staff to gain an understanding of the process or procedures taken to validate that appropriate security controls are in place for the cloud computing environment. Determine if the following services existed for cloud computing: intrusion detection, virus protection, malware prevention and vulnerability scanning.

Internet2 and net+ Contracts:
Reviewed systemwide initiatives related to Internet2. Gained an understanding of the current status of the Internet2 agreement and business analysis required to determine if Internet2 offers the best option.

IT Cloud Services Purchased with a Pro-Card:
Reviewed SQL report of Pro-Card statements and searched for a list of known cloud service providers. Scanned and reviewed Pro-Card statements related to cloud services. Determined if substantive risks are created with Pro-Card use.

Business Criticality in IT Cloud Contracts:
Discussed concept of business criticality with UCSC staff, UCOP staff and legal counsel. Determined if business criticality needs to be a second factor (in addition to data classification) to drive contract requirements.

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A.	IT Cloud Services Business Contracting	
Opportunities were identified for strengthening IT cloud service contracts by implementing steps to improve assurances on client reported data classification levels and by considering business criticality when establishing agreement requirements.		
Risk Statement/Effect		
Effective IT cloud service contracts and contracting processes help provide assurance that that data will be appropriately secured and that cloud service providers have controls in place to prevent data breaches, loss of data or breakdown of data integrity, or loss of system or business functionality.		
Agreements		
A.1	Procurement Services will collaborate with the Chief Information Security Officer (CISO) and the Privacy and Information Practices Coordinator to design and implement a formal process enabling campus departments to effectively contract for IT cloud computing services provided by an external supplier. The process will be expected to address the following areas: a. Provide guidance to departments seeking external IT cloud computing services covering things such as data classification and related security requirements, restricted and confidential data protection standards, and cloud computing alternatives b. Define the responsibilities of parties involved in the process, including the requesting department and central offices, c. Identify the factors, including business criticality, to be used to determine the security-related terms and conditions that are to be included in a purchase order or contract. d. Provide for verification of the proper classification of data expected to be maintained on a supplier's system so the appropriate contracting terms and conditions are included in the purchase order or contract issued to the supplier. e. Implement tools, such as forms, checklists, and/or "decision trees" to facilitate and document the data verification process.	Implementation Date 1/15/17 Responsible Managers • Procurement Services Director* • Chief Information Security Officer • Privacy and Information Practices Coordinator *will assume responsibility for reporting on progress of the effort
A.2	For agreements processed by the Business Contracts Office, which contain confidential or restricted data, Procurement Services will include Appendix DS as an attachment to the agreement and not as a web link.	Implementation Date 3/31/16 Responsible Manager Business Contracts Manager

A.3	Procurement Services in consultation with the Office of the Chief Information Security Officer will establish guidelines for the campus departmental clients to monitor IT cloud agreements.	Implementation Date 1/15/17 Responsible Manager • Procurement Services Director* • Chief Information Security Officer *will assume responsibility for reporting on progress of the effort

A. IT Cloud Services Business Contracting – Detailed Discussion

Cloud service providers manage both data and services on behalf of the University. Cloud computing agreements are the only means to assure University data is stored, transmitted and managed in a secure manner that facilitates University business processes. The agreements established with these companies must align to the campus practices and policies established for data confidentiality, integrity, availability, and risk management. UCSC has no direct control over the data after it has been saved to the cloud. The University does not have a policy, model agreements or appendices written specifically for cloud computing. Procurement Services takes on an enormous amount of responsibility to assure the University's data is protected and the services agreed to meet its business needs.

Data Classification used to Determine Agreement Requirements

Data classifications, specifically confidential and restricted data, are the primary factors to determine the required content and risk assessments for IT cloud agreements. End users provide data classification information in the CruzBuy requisition and are considered responsible for the accuracy of the information. The campus provides public information about data security, but these end users have not received any focused training related to data classification. As part of their simplification initiatives, Procurement Services senior management strongly advised Procurement Services employees and buyers to not ask end users questions about data classification. However, as data classification represents one of the greatest risks in cloud computing, it may be advisable to re-examine this practice.

End User Information Related to Agreement Process

Procurement Services is developing an end user business contracts guide that will help to educate end users and provide references so they better understand concepts, like restricted and confidential data, among other things they need to know in order to create requisitions in CruzBuy.

There are a number of on-line forms in CruzBuy that are used to help guide users through specific procurement requirements. Answering questions contained within these forms is required to complete a requisition in CruzBuy. The form most commonly used for cloud agreements is the one-page "Services" form. This form asks basic questions such as the catalog number, product description, quantity, estimated price and begin and end dates. All the other questions on this form are related to conflict of interest issues that apply largely to service providers.

An opportunity exists to develop a CruzBuy form that is specifically geared to address requirements unique to an IT cloud service agreement, such as information about restricted or confidential data classification and business criticality.

We encouraged Procurement to develop such a form. Buyers in Procurement often have to instruct end users to address data classification issues, so they have to go back and modify the form already completed, which is a duplication of effort. Procurement cited a lack of resources as a reason to not develop a new form. We did not agree but deferred to Financial Affairs for taking alternative action to address education and assurances over data classification and business continuity with end users when contracting with an IT cloud service provider.

Procurement Services' Role

Until recently, if Procurement Services reviewed an agreement that implied that restricted or confidential data might be involved but was not disclosed, they would talk to groups on campus with expertise in specific areas, such as Infrastructure Security, Privacy and Information Practices, Controllers Office (PCI), Campus Counsel or Student Health Center (HIPAA), Risk Services (cyber liability insurance) and end users to determine the legitimacy of this potential and its impact. This action represented a best effort to mitigate potential risk. However, a recent directive to simplify procurement processes increased the risk to the University by eliminating further inquiry, asserting that the end users are responsible for being aware of data classification risk, and not inquiring further into data classification levels. Procurement Services has continued to document the discussions regarding data classification in the CruzBuy requisition. The end user is the only official control point to assure these types of data are identified. Proactive inquiry as to data classification type from Procurement Services and ITS would be prudent. In addition, use of a standard decision tree and checklist would go a long way in assuring restricted and confidential data are identified before agreements are completed.

Use of UC Data Security and Privacy (Appendix DS) and Related Processes at UCSC

The desired position of the University is to get suppliers to accept the University Appendix DS as part of the IT cloud agreement. If the supplier agrees to create, receive, maintain or transmit confidential or restricted data on behalf of the UC, the supplier shall be bound by the obligations set forth in the University of California Appendix - Appendix DS. In cases where the supplier will not agree to include Appendix DS or suggests a red-lined version, the UCSC Office of the Chief Information Security Officer (CISO) has developed a Supplier Safeguard form and process to determine if the supplier provides commensurate controls and/or a business risk assessment is performed to determine that an agreement is acceptable without Appendix DS. The Office of the CISO documents this analysis and the recommendation to proceed or not in the requisition.

The supplier safeguard process was developed six months ago, so it is too early to confirm its full adoption as an on-going process. Many cloud service vendors begin the agreement process by supplying their own standard agreement language which is red-lined back and forth during the negotiation process. They may insist that any changes are made in this manner, rather than inserting the full Appendix DS. For example, the AWS agreement does not include the Appendix DS, but the negotiated agreement was deemed to contain sufficient data security elements. The Supplier Safeguard process also includes steps for the supplier to provide third-party audit reports such as AICPA SOC 2, ISO certification, PCI certification or similar reports. The CISO has final authority to accept or reject agreements in this scenario.

If a cloud system will contain confidential data, Appendix DS is also required, but if it is not included in the agreement, or red-lined, the Office of the CISO uses an Alternate Language Matrix to compare the controls in the supplier's agreement to Appendix DS. The client will use this comparison to determine if it is appropriate to complete the agreement.

Appendix DS Included in Agreement via Web Link

One cloud agreement we reviewed that was executed in 2012 included Appendix DS by a link to a URL on the UCOP website. When we reviewed the agreement in 2015, the URL was a broken link because Appendix DS had been reissued multiple times with new URL's each time. The old copy that was included in this agreement is not maintained and may be difficult to obtain. It will likely require advice from legal counsel to determine what effect the broken link has on the agreement validity.

On-going Monitoring

UCSC does not provide on-going monitoring of cloud service provider status or the agreements associated with them. Procurement Services informed us that other UC campuses with larger agreement offices perform this function. For example, if security controls maintained by an IT cloud services provider were to change, the campus would not have an established method to detect or make changes to the process or agreement. Reviewing subsequent third party reviews, such as a SOC 2/3, after the initial year the agreement was entered into is one way to provide on-going monitoring. In the case where Appendix DS was referenced as a web link that was later broken on-going monitoring could have triggered appropriate follow-up. The full legal implications of having an agreement with only a broken web link are not known.

Business Criticality

When we discussed cloud computing risks with the Senior IT commodity manager in Procurement at UCOP, he noted the two most important factors for cloud agreements were data classification and business criticality. UCSC does not consider business criticality in drafting contracts with IT cloud service providers. As noted in the prior section, data classification is the primary consideration for cloud computing agreements and drives specific requirement such as the use of Appendix DS. When we asked UCOP for a definition of business criticality no specific examples were provided, but it was stated that it would likely apply anytime someone stores the only copy of critical data in the cloud. Business and Finance Bulletin IS-12 further defines criticality as a measure of the importance of a resource to the functional operation of a campus or department and the priority of that function in continuity plans and disaster recovery strategies.

The controls that should be included for business critical systems include data backups and ownership, availability and source code escrow or others means to obtain data portability. We reviewed data backup strategies in the five cloud computing agreements reviewed and found that two of these suppliers state they keep backups for seven days; one said they keep backups for 14 days; two did not specify backup retention periods. No local backups of cloud computing data are maintained. UCSC appears to own its data on all systems reviewed although this was only specifically stated on three of five agreements reviewed. Only one of the five agreements reviewed specified system availability at 99%, although availability problems have not been reported for the other systems. Only one of the five agreements reviewed included application source code escrow. Due to the complexity of modern databases, if a cloud service application became unavailable the data in the database alone would likely be unusable for university business purposes. Source code escrow provides that if the company can no longer provide the service the source code would be available so the application could be run locally. The CISO noted it may not always be possible for the campus to compile source code and run the application locally, but for essential systems, some means to obtain usable data portability will be needed if the supplier no longer provides the service.

If it is decided that business criticality should be a factor in formulating cloud computing agreements, it may be a good practice to review independent audit reports to assure the controls function as intended such as a SOC, ISO certification, or similar independent audit reports to assure the supplier's controls function as intended.

Agreement Templates

Systemwide Procurement prefers to incorporate the University's standard terms and conditions into all agreements, but most cloud service suppliers will only negotiate agreements based on their standard agreement language, which is red-lined to make any needed changes. Procurement Services attempts to assure terms related to important issues such as indemnification, insurance and data security are acceptable to the risk profile of the University, but it is often not possible to include all the University's terms and conditions and it simply does not happen in most cases.

A system-wide group coordinated by the senior IT commodity manager at UCOP Procurement produced a draft 37-page cloud computing agreement template in 2011, although it was never officially sanctioned by UCOP. UCOP Procurement has published a number of agreement templates, but there is no requirement for the campuses to use the templates. UC Irvine attempted to use the cloud template draft, but after much work, they were unsuccessful in obtaining a signed agreement. UCOP is in the process of creating a new cloud agreement template, but since most successfully negotiated agreements are based on supplier provided language it is unclear how this new template will be used. It may best serve as a checklist to assure all important issues are addressed.

Internet2 Consortium

Internet2 is a non-profit United States-based computer networking consortium led by members from the research and education communities, industry, and government. Internet2 has over 500 member institutions, including 251 institutions of higher education (including UC). The Internet2 Network, through its regional network and connector members, connects over 90,000 U.S. educational, research, government and "community anchor" institutions, from primary and secondary schools to community colleges and universities, public libraries, museums and health care organizations. The Internet2 community develops and deploys network technologies for the future of the Internet.

The products and services offered by the Internet2 consortium include:

- Advanced networking
- Cloud services and applications
- Trust, identity and middleware
- Performance and analytics

For cloud services, Internet2 executes an agreement with the cloud service provider on behalf of the member institutions. When a member institution wants to use one or more cloud services they pay Internet2 for the services and not the third party cloud provider. The idea being this would provide greater efficiency and cost savings since each institution would not have to negotiate terms and conditions with the supplier. This could help to reduce the workload on Procurement Services and would provide the campus with faster secure access to the needed cloud services. Unfortunately, at the time of our review, Internet2 had executed a master agreement with the UC system, but the suppliers were unwilling to accept the conditions under this master agreement. Internet2 will continue to work with UCOP and the suppliers to try to negotiate the areas of disagreement with the suppliers. For now, we have no option but to continue to utilize the existing system-wide agreements and execute local agreements as needed.

B.	Cloud Governance and Guidance	
IT cloud services governance and supplier management is immature, and lacks an overriding systemwide or campus policy and guidance for acquiring and or administering new IT cloud computing services. The campus does not have a means to provide advice or guidance about cloud service providers to end users who choose to use instructional or administrative cloud computing services.		
Risk Statement/Effect		
Users are unable to evaluate and make appropriate choices regarding IT cloud services if they lack guidance and education related to data classification, business criticality and general cloud technology.		
Agreements		
B.1	ITS will continue developing the instructional cloud computing web project to inform users of risks and appropriate choices of IT cloud service providers.	Implementation Date 12/23/16 Responsible Managers Faculty Instructional Technology Center Operations Manager
B.2	ITS will consider developing a cloud computing risk matrix for other non-contracted commonly available cloud service applications based on the model developed in the instructional cloud computing web project.	Implementation Date 7/1/16 Responsible Managers Chief Information Security Officer

B. Cloud Governance and Guidance – Detailed Description

Use of third party IT cloud services is a rapidly growing phenomenon. IT cloud services can be obtained in a variety of ways by campus faculty and staff: through University acquired contracts such as the Amazon Web Services (AWS) agreement; supplier agreements obtained by out of pocket (reimbursed) or Pro-Card; or by "click-through" agreements used for free cloud services.

ITS provides guidance for campus faculty and staff who need help establishing a cloud storage services solution using the campus cloud provider AWS, or on-premises storage solutions within the Data Center. ITS also provides information and guidance to users, telling them to not transmit and store unencrypted restricted data on cloud services. Otherwise, there is little in the way of education, policy or specific guidance for end users who have the freedom to use cloud services without the benefit of UC contracts. Training, risk review and approval processes are lacking, but could be incorporated into the instructional cloud computing web page and cloud computing risk matrix as part of that project. As more information is obtained about these IT cloud providers, it may become more feasible to develop useful policy statements such as when approvals to use cloud services may be needed

to mitigate risks. Currently, the overall cloud infrastructure is immature and includes so many unknown factors that rational policy may be difficult to develop and administer.

The campus has not assigned responsibility to maintain an inventory of cloud services and does not actively monitor cloud use due to restrictions in the Electronic Communications Policy. It may not be practical to have a complete inventory as cloud service providers are constantly changing and there are no restrictions on cloud use. However, an inventory of cloud service providers with active agreements may be beneficial so that these providers and agreements can be better monitored. The fact that the campus is unaware of all the cloud services in use is a risk, but given the current academic environment, there may not be a viable way to mitigate this risk.

Some campuses have begun a process for reviewing and recommending selected IT cloud providers for use at their respective campuses. For example, UC Irvine has a website for instructional cloud computing that lists the characteristics, risks and recommendations for use for the ten most commonly used instructional cloud service providers. Refer to Appendix C. Each provider is rated on functionality, privacy, student records, security, legal and contract (if a contract is in place). Each of these review factors are rated on a four-point scale so that faculty can make informed decisions about which one will work for their class and what types of data are reasonable to use.

UCSC has just begun work on an instructional cloud computing web project that is intended to produce a web page that will provide detailed information on cloud computing services commonly used by faculty in support of the courses they teach, as well as a means to host streaming space audio and video files used by students as part of their course work.

C.	Assurances of IT Cloud Service Provider Maintained Controls	
Assurances of the existence and adequacy of internal controls maintained by IT cloud service providers was not always obtained prior to releasing data or receiving IT cloud services.		
Risk Statement/Effect		
Entering an agreement with an IT cloud services provider without a third party assessment of their control systems places campus data at risk.		
Agreement		
C.1	Procurement Services will collaborate with the Chief Information Security Officer (CISO), and the Privacy and Information Practices Coordinator to establish an appropriate process to require a SOC 2 or 3 or similar third party report on controls, as a condition of entering into all IT cloud computing services agreements for assurance of adequate security controls. The process should identify the appropriate approval responsibly that assumes responsibility in those cases were a third party report is not available or cannot be obtained.	Implementation Date 1/15/17 Responsible Managers • Procurement Services Director* • Chief Information Security Officer • Privacy and Information Practices Coordinator *will assume responsibility for reporting on progress of the effort

C. Assurances of IT Cloud Service Provider Maintained Controls – Detailed Description

There are several ways to help ensure that third-party providers of IT cloud services have sufficient working controls in place to protect the integrity and security of the University's data entrusted to them. In addition to including requirements in the agreement, some options available include conducting or contracting for specific IT audits and reviews of the IT cloud provider control systems; relying on external reviews and certifications provided by those with the required knowledge, skills and credentials using industry standards.

SOC 2 and SOC 3 IT service provider certification reports are designed to meet the needs of users who want assurances that the controls at a service organization are in place and functioning as intended. These reports use the AICPA trust services principles, and criteria specifically designed to help users understand the internal controls in a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. SOC 2 reports include details on the service provider's controls as well as the auditor's detailed test procedures and test results. SOC 3 reports provide an overall conclusion on whether the service provider achieved the stated trust services criteria (internal controls) and the user does not need to understand the detailed control descriptions and test procedures. SOC 3 reports are intended to be freely distributed and may be displayed on a service provider's website. Cloud service providers are not required to obtain SOC 2 and SOC 3 reports, although the most reputable providers likely have these reports. In addition, when applicable, other standards or certifications

such as PCI DSS (for credit cards), HIPAA (for health information), and ISO 27002 may provide necessary assurances.

For agreements involving systems containing credit card or protected health information, the current contracting protocols require PCI DSS or HIPPA Security Rule compliance as a condition of the agreement which all provide strong assurance the suppliers meet external review requirements and comply with industry standards.

The CISO has recently developed the supplier safeguard process that invokes a risk assessment whenever Appendix DS is not included in the agreement while restricted data is present, together with the alternative language matrix when confidential data is present. The supplier safeguard process included a step to review for the existence of a SOC 2/3, ISO or PCI or similar reports as applicable. The CISO conducts these reviews independently of Procurement Services, although the results are documented in the CruzBuy requisition.

However, a requirement that a SOC 2 or a SOC 3 report be included in the agreement as a condition for contracting with all or a select subgroup of IT cloud service providers could be established. At a minimum, a SOC 3 report should be required on those IT cloud service providers providing business critical services. The added effort to administer this requirement would likely be minimal. In the unlikely event that a SOC 2/3 report identifies a control weakness or the report is not available, the agreement could be canceled or a more detailed review involving the CISO could be performed.

APPENDIX A – NIST Special Publication 800-145 – The NIST Definition of Cloud Computing

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

Cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

1.3 Audience

The intended audience of this document is system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services.

2. The NIST Definition of Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[2]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.[3] The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

[1] Typically this is done on a pay-per-use or charge-per-use basis.

[2] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

Deployment Models:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Source: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

APPENDIX B – UC Data Security and Privacy (Rev. 10/27/14) "Appendix DS"

UNIVERSITY OF CALIFORNIA

APPENDIX – DATA SECURITY AND PRIVACY

ARTICLE 1 – PURPOSE AND SCOPE OF APPLICATION

A. This Data Security and Privacy Appendix is designed to protect the University of California's (UC) Protected Information and UC networks (defined below). This Appendix describes the data security and privacy obligations of all third parties (including individuals and entities) that connect to UC networks and/or gain access to Protected Information (Supplier).

B. Supplier agrees to be bound by the obligations set forth in this Appendix. To the extent applicable, Supplier also agrees to impose, by written contract, the terms and conditions contained in this Appendix on any third party retained by Supplier to provide services for or on behalf of the UC.

ARTICLE 2 – PROTECTED INFORMATION

A. Supplier acknowledges that its performance of Services under this Agreement may involve access to confidential UC information that identifies or is capable of identifying a specific individual, including, but not limited to, personally-identifiable information, student records, protected health information, or individual financial information (collectively, "Protected Information") that is subject to state or federal laws restricting the use and disclosure of such information, including, but not limited to, Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civil Code § 1798 *et seq.*); the California Confidentiality of Medical Information Act (Civil Code § 56 *et seq.*); the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164); the federal Fair and Accurate Credit Transactions Act (15 USC § 1601 *et seq.*) and the Fair Credit Reporting Act (15 USC § 1681 *et seq.*); the European Union Data Protection Directive and other state, federal and international laws.

B. All Work Product, works-in-progress, notes, data, reference materials, memoranda, documentation and records in any way incorporating or reflecting any of Protected Information and all proprietary rights therein, including copyrights, will belong exclusively to the UC and unless expressly provided, this Appendix will not be construed as conferring on Supplier a license or option for a license any patent, copyright, trademark, license right or trade secret owned or obtained by UC.

ARTICLE 3 – ACCESS TO UC NETWORKS

"UC networks" means the set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information that is implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. Examples of networks include local area networks (LAN), wide area networks (WAN), Storage area networks (SAN), Enterprise private networks (EPN), Virtual private networks(VPN), Wireless local area networks (WLAN), or Campus area networks (CAN).. UC networks include resources that are purchased, leased and/or otherwise obtained for use by UC, and may include personally owned devices. In any circumstance when Supplier has access to UC networks, it is the sole responsibility of Supplier to ensure that its access to the networks does not result in any access by unauthorized individuals to UC networks or Protected Information. This includes access to all types of UC network logins or credentials, as well as access to information contained on or transmitted through those networks. It is Supplier's sole responsibility to protect the login and credential information, including through proper use, handling and destruction of such information. Consistent the requirements in Attachment 1, any technology and/or systems that gains access to UC networks must comply with the Computer System Security Requirements.

Rev. 10/27/2014 Page 1 of 7

Source: http://www.ucop.edu/procurement-services/_files/appendix-data-security.pdf

APPENDIX C – ITS Website – Amazon Web Services

Self Service Cloud Computing

Self Service Cloud Computing allows UCSC faculty, staff, and students (with a faculty/staff sponsor) to order, provision, and use computing resources from an approved cloud services provider. That approved provider for UCSC is Amazon Web Services.

On This Page

- AWS Services Available
- Costs
- Sign up for AWS Cloud Computing
- More Information
- AWS Contract
- AWS Support

The University of California has negotiated a contract with **Amazon Web Services (AWS)** that includes acceptance of UC terms and conditions. This contract has a unique set of terms and conditions that are specific only to the University of California campuses. In addition, Amazon Web Services is allowing the procurement of services using a UC purchase order via CruzBuy. You will signup for an account with AWS, get your purchase order through CruzBuy, and activate your account with your purchase order. AWS will provide invoices to your email address. View AWS Contract

Amazon Web Services Available

For the complete and current list of services available, please visit Amazon Web Services

- **Amazon Elastic Compute Cloud** delivers scalable, pay-as-you-go compute capacity in the cloud. More information
- **Auto Scaling** allows you to automatically scale your Amazon EC2 capacity up or down according to conditions you define. More information
- **Amazon Elastic Block Store** provides block level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are off-instance storage that persists independently from the life of an instance. More information
- **Amazon Simple Storage Service** provides a fully redundant data storage infrastructure for storing and retrieving any amount of data, at any time, from anywhere on the Web. More information
- **Amazon CloudWatch** provides a monitoring system that will estimate Amazon Web Service charges. More information
- **Amazon Web Service Support** offers one-on-one support that operates 24/7 by Amazon's technical support engineers. AWS support also offers different levels of support. More information

Costs

With Cloud Services, you pay for what you use; for most services, there is no minimum fee. The AWS monthly cost calculator can show you the estimated monthly cost of various services and configurations: Cloud Service Calculator

AWS also offers a free usage tier!
To learn more about this program and to understand its limits, visit: AWS Free Usage Tier

Except for the free usage tier, AWS charges for use of their services, usually by the hour or any part of an hour that a service is used. Amazon also charges for the bandwidth used for data transfer between their services and the Internet. AWS provides many different price tiers, and many ways to reduce your costs.

Managing the usage of AWS resources on an ongoing basis is very important to managing your costs. Pricing for each service is listed on the AWS website.

Sign up for Self Service Cloud Computing

You can set up your AWS account using either a UCSC Pro-Card or Purchase Order. You might want to consult with your local financial person to see if they have a preference; either method will require processing a monthly bill.

Both the Purchase Order method (automatically) and the Pro-Card method (by request) can be covered by the University of California terms and conditions. The workflow for each method is defined below.

Ordering AWS services: Workflow for Purchase Order

- Determine the dollar amount of your PO and the FOAPAL you want to use.
- Sign up for an account at this special AWS site: Sign up for AWS -- Instructions on How to Sign Up (PDF)
- Be sure to use your @ucsc.edu email address.
  - ***NOTE:*** *If you use your UCSC account for your personal Amazon.com account, you will want to change that email address to a non-ucsc account on your personal Amazon.com account. You may also use a plus in the account address, for example cruzid+aws@ucsc.edu for your AWS account.*
- AWS will assign you a twelve-digit account number; be sure to make a note of it.
- Create a requisition in CruzBuy using the Blanket PO Request form, including your AWS twelve-digit account number as an external note.
- Procurement will review and approve the requisition, then create a purchase order and distribute it to AWS. This provides AWS with the information required to set up the account for PO invoicing.
- AWS will set up the account up for PO invoicing, and confirm when your account is ready to go. This confirmation will be sent to the email address that was used to set up the account. This may take a couple of days after the PO has been issued.

- Each month, AWS will send an invoice to FAST, and FAST will pay AWS.
- Workflow tips:
  - If you have more than one account, or want to track or pay for different services with different FOAPALs, it is recommended that you set up a separate PO for each.
  - If this is for a long-term project:
    - Determine the dollar amount for the current fiscal year spend
    - Place this amount on one PO line
    - If you expect to span to the next fiscal year, add a second PO line at $10, as a placeholder to keep the PO open
  - Need more help? Contact your Procurement Buyer Service Team (https://financial.ucsc.edu/Pages/Purchasing_Contacts.aspx) for more information about ordering AWS services.

Ordering AWS services: Workflow for Pro-Card

- Sign up for an account at the standard AWS site: Standard Registration
- Be sure to use your @ucsc.edu email address. You will also need to enter your Pro-Card information and bill-to address.
- Send an email to aws-uc-procurement@amazon.com to request that your account should be covered by the UC AWS Enterprise Agreement terms. Your email must include your AWS twelve-digit account number.
- Each month, AWS will charge your Pro-Card but will not send a detailed invoice; you can get these details through the AWS management console, and set up billing alerts there as well.

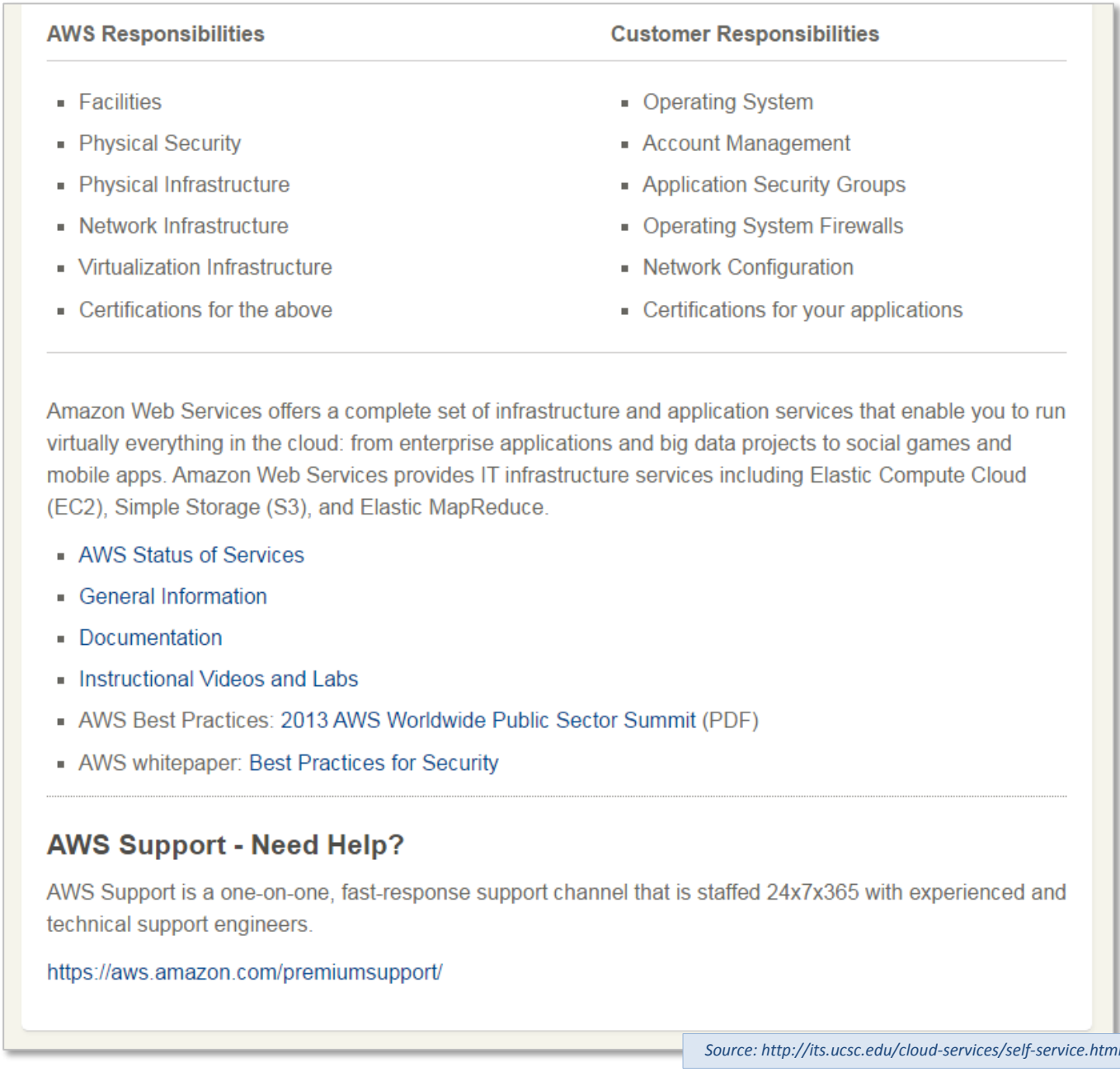
More Information About Amazon Web Services

Shared Security Model at AWS

AWS has a "shared responsibility model" for information security and compliance. Because you're building systems on top of the AWS cloud infrastructure, the security responsibilities will be shared: AWS has secured the underlying infrastructure and you must secure anything you put on the infrastructure.

This means that there are several security decisions you need to make and controls you must configure. For information on how to configure a particular AWS service, see the documentation for that service. For more tips on security with AWS, check out the AWS Security Center.

If you're not comfortable taking on these responsibilities, consult with your ITS Divisional Liaison or consider using the Managed Cloud Services model instead.



AWS Responsibilities	Customer Responsibilities
▪ Facilities	▪ Operating System
▪ Physical Security	▪ Account Management
▪ Physical Infrastructure	▪ Application Security Groups
▪ Network Infrastructure	▪ Operating System Firewalls
▪ Virtualization Infrastructure	▪ Network Configuration
▪ Certifications for the above	▪ Certifications for your applications

Amazon Web Services offers a complete set of infrastructure and application services that enable you to run virtually everything in the cloud: from enterprise applications and big data projects to social games and mobile apps. Amazon Web Services provides IT infrastructure services including Elastic Compute Cloud (EC2), Simple Storage (S3), and Elastic MapReduce.

- AWS Status of Services
- General Information
- Documentation
- Instructional Videos and Labs
- AWS Best Practices: 2013 AWS Worldwide Public Sector Summit (PDF)
- AWS whitepaper: Best Practices for Security

AWS Support - Need Help?

AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced and technical support engineers.

https://aws.amazon.com/premiumsupport/

Source: http://its.ucsc.edu/cloud-services/self-service.html

APPENDIX D – UC Irvine – IT Cloud Services Provider Ratings

UCI Instructional Cloud Computing

Search

Home | Review Process | Review Criteria | Tools & Services | About Us

Tools & Services

The directory below provides a high-level summary of the tools that have been reviewed or are in progress. We recommend reading through the Rating Descriptions for an explanation of the icons used in the table. We also suggest you read the full review for any tool you are interested in using. If the tool you have in mind has not been reviewed yet, check our Planned Reviews for a list of the tools currently in our queue. Better yet, help us prioritize our list by letting us know which tools you are interested in using or what types of functionality you need.

Name	Typical Uses	Functional	Privacy	Student Records	Security	Legal	Contract
Doceri Read Full Review	▪ Conduct your lecture as you interact with the students in the classroom ▪ Annotate PowerPoint presentations during your in-class session	✓	!	!	!	–	☆
Google Apps (UCI) Read Full Review	▪ Have student groups collaboratively create a presentation ▪ Collaboratively write a research paper or article for publication	✓	✓	✓	✓	✓	★
Google Hangouts (UCI) Read Full Review	▪ Conduct online office hours ▪ Encourage student groups to collaborate synchronously	✓	✓	✓	✓	✓	★
Kahoot! Read Full Review	▪ Check for understanding during classroom lectures ▪ Engage the students in a competitive "quiz"	!	✓	✓	✓	–	☆
Piazza Read Full Review	–	!	✗	!	!	✗	–
Poll Everywhere Read Full Review	▪ Gauge understanding of a topic within a lecture ▪ Encourage participation in a real-time poll from an audience	✓	✓	✓	!	–	☆
ProctorU Read Full Review	▪ Verify the identity of a student completing an online assessment ▪ Schedule time for a student to visit a physical location and complete an assessment in a managed environment	✓	–	–	–	–	★
Sapling Learning Read Full Review	▪ Create, deliver, and grade online homework	✓	!	✗	✗	!	☆
Scribblar Read Full Review	▪ Conduct online office hours ▪ Provide web-based interactive tutoring sessions	✓	✗	✓	✗	–	☆
VoiceThread (Self Sign-Up) Read Full Review	▪ Discuss topics using voice and video asynchronously ▪ Online student presentations	✓	✗	!	✗	–	☆
Zaption Read Full Review	▪ Add questions to online videos ▪ Track viewership of online videos	!	✗	!	✗	–	☆

Icon Key (read full descriptions)

Review Status		Contract Status	
✓	Recommended for use	★	Contract in place
!	Use with caution	★	Negotiations underway
✗	Not recommended	☆	Qeued
–	In progress	☆	Not planned

Source: http://sites.uci.edu/cloud/directory/

APPENDIX E – Google Service Organization Control (SOC) 3 Report

Service Organization Control (SOC) 3 Report

Report on the Google Apps for Business & Education, Other Google Services & Google Cloud Platform (System) Relevant to Security, Availability, Processing Integrity, and Confidentiality

For the Period May 1, 2013 to April 30, 2014

1600 Amphitheatre Parkway
Mountain View, California 94043

Tel: 650.623.4000
Fax: 650.618.1806
www.google.com

Google's Management Assertion Regarding the Effectiveness of Its Controls Over the Google Apps for Business & Education, Other Google Services, and Google Cloud Platform (System) Based on the Trust Services Principles and Criteria for Security, Availability, Processing Integrity, and Confidentiality

Google Inc. maintained effective controls over the security, availability, processing integrity and confidentiality of its Google Apps for Business & Education, Other Google Services, and Google Cloud Platform (System) to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification;
- the System was available for operation and use, as committed and agreed;
- the System processing was complete, accurate, timely, and authorized; and
- the System information designated as confidential was protected as committed or agreed

during the period May 1, 2013 through April 30, 2014 based on the security, availability, processing integrity, and confidentiality principles set forth in the AICPA's TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Our attached System Description of the Google Apps for Business & Education, Other Google Services, and Google Cloud Platform (System) identified the aspects of the System covered by our assertion.

GOOGLE Inc.

July 16, 2014

1

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110
Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Building a better working world

Report of Independent Accountants

To the Management of Google Inc.

We have examined management's assertion that Google Inc., during the period May 1, 2013 through April 30, 2014, maintained effective controls to provide reasonable assurance that:

- the Google Apps for Business & Education, Other Google Services, and Google Cloud Platform (System) was protected against unauthorized access, use, or modification;
- the Google Apps for Business & Education, Other Google Services, and Google Cloud Platform (System) was available for operation and use, as committed and agreed;
- the Google Apps for Business & Education, Other Google Services, and Google Cloud Platform (System) processing was complete, accurate, timely and authorized; and
- the Google Apps for Business & Education, Other Google Services, and Google Cloud Platform (System) information designated as confidential was protected as committed or agreed

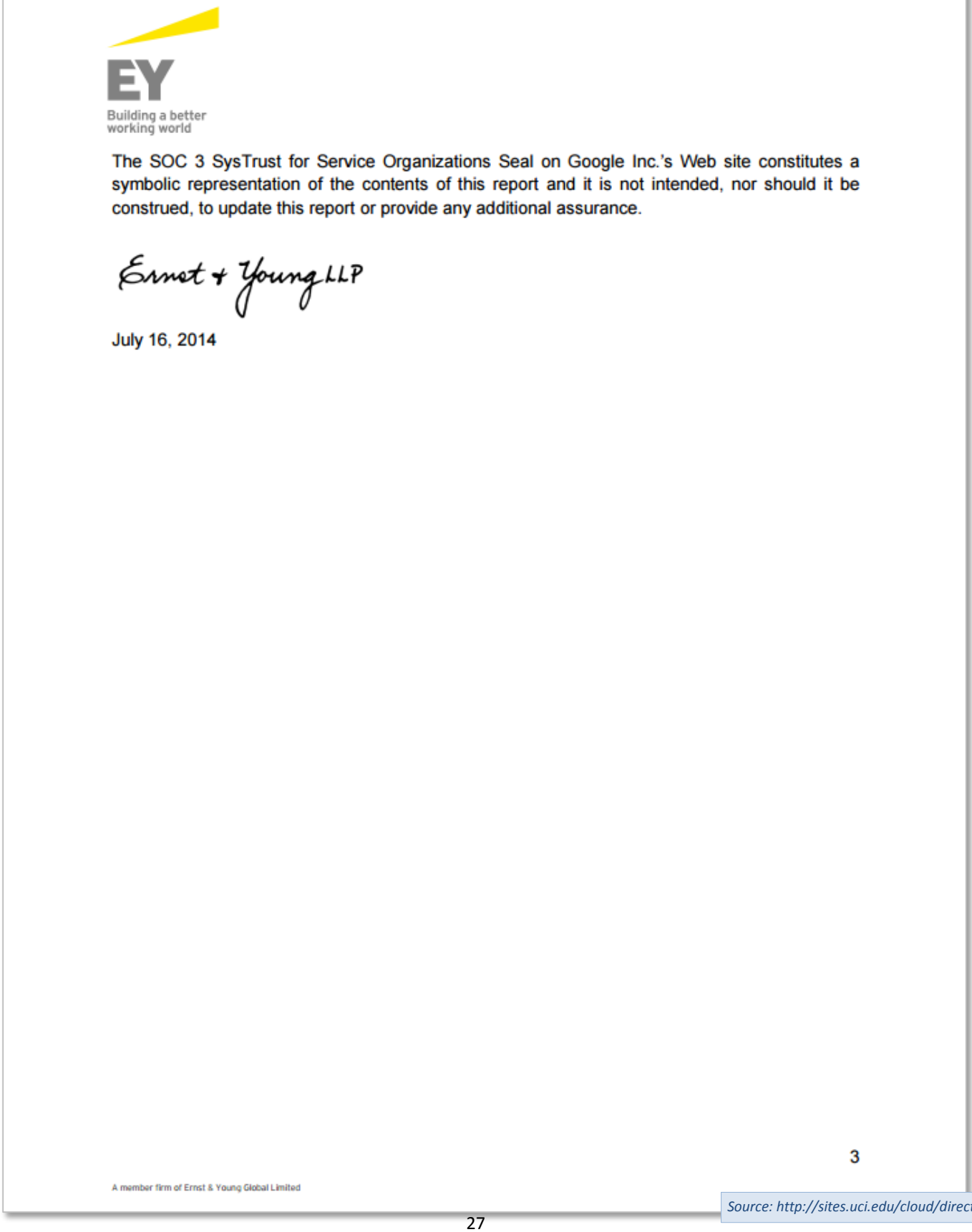
based on the security, availability, processing integrity, and confidentiality principles set forth in the AICPA's TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Google Inc.'s management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Google Inc.'s relevant security, availability, processing integrity and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations of controls error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls the failure to make needed changes to the system or controls or a deterioration in the degree of the effectiveness of the controls.

In our opinion, Google's management assertion referred to above is fairly stated, in all material respects, based on the AICPA/CICA Trust Services™ Security, Availability, Processing Integrity and Confidentiality Criteria.

2



EY
Building a better working world

The SOC 3 SysTrust for Service Organizations Seal on Google Inc.'s Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Ernst + Young LLP

July 16, 2014

3

A member firm of Ernst & Young Global Limited

Source: http://sites.uci.edu/cloud/directory/