UCSB Audit and Advisory Services

Internal Audit Report

Third Party IT Services

August 1, 2014

Performed by:
Antonio Manas-Melendez, Senior Auditor

Approved by:
Robert Tarsia, Director

Report No. 08-14-0014

This page intentionally left blank.

University of California, Santa Barbara

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

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
SANTA BARBARA, CALIFORNIA 93106-5140
Tel: (805) 893-2829
Fax: (805) 893-5423

August 1, 2014

To: Denise Stephens
Interim Chief Information Officer
Enterprise Technology Services

Distribution

Re: **Third Party IT Services**
Audit Report No. 08-14-0014

As part of the 2013-14 annual audit services plan, Audit and Advisory Services has completed an audit of the use of third party IT services at University of California, Santa Barbara (UCSB). Enclosed is the report detailing the result of our review.

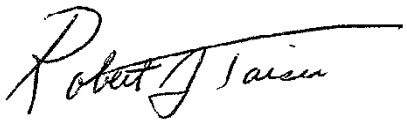
The purpose of this review was to determine if there are adequate controls over, and monitoring of, decentralized department and "casual" use of third party IT services without the supervision of UCSB IT departments.

The result of our work indicate that existing policies, procedures, and guidelines are not sufficient to help ensure the protection of University data and compliance with laws, regulations, and UC policies. There is a need for the campus to address the risks associated with the use of third party IT services by developing, vetting, and issuing a campus policy covering the purchase and use of third party IT services, along with more detailed procedural and other guidance. There are also immediate opportunities to promote campus best practices and to mitigate risks in advance of the development and approval of campus policies and procedures, including web-based guidance and educational efforts to help the campus community to understand the risks of these services and best practices to reduce those risks. We noted that some UC campuses have implemented and communicated relevant guidelines to their campus communities.

Detailed observations and management corrective actions are included in the following sections of the report. The management corrective actions provided indicate that each audit observation was given thoughtful consideration and positive measures have been taken or planned in order to implement the management corrective actions.

The cooperation and assistance provided by Enterprise Technology Services and many other campus personnel during the review was sincerely appreciated. If you have any questions, please feel free to contact me.

Respectfully submitted,



Robert Tarsia
Director
Audit and Advisory Services

Enclosure

Distribution:

Enterprise Technology Services
Sam Horowitz, Chief Information Security Officer
Doug Drury, Director Business Relationship Management
Bruce Miller, Associate Director of Technology
Mathew Dunham, Associate Director Identity & Cloud Services
Mike Tornquist, Operational Data Store Administrator

Administrative Services
Jim Corkill, Controller and Director, Business & Financial Services
Leslie Griffin, Associate Director, Business & Financial Services
Jacob Godfrey, Associate Director and Materiel Manager, Business and Financial Services
Ben Price, Director, Information Systems & Technology, Housing - Information Systems

Alan Moses, Assistant Dean for Academic Technology, College of Letters & Science
May Chang, Associate University Librarian, Information Technology & Digital Initiatives, University Library
Jim Wood, Director of Computing, Marine Science Institute
Richard Kip, Assistant Director ECI, College of Engineering

cc: Chancellor Henry Yang
Interim Executive Vice Chancellor Joel Michaelsen
Senior Associate Vice Chancellor Marc Fisher, Administrative Services
UCSB Audit Committee
Senior Vice President and Chief Compliance and Audit Officer Sheryl Vacca

UCSB Audit and Advisory Services
Third Party IT Services
Audit Report No. 08-14-0014

PURPOSE

The primary purpose of this audit was to determine whether University of California, Santa Barbara (UCSB) has adequate controls over, and monitoring of, decentralized department use of third party information technology (IT) services. This audit is part of the fiscal year 2013-14 audit services plan of UCSB Audit and Advisory Services.

SCOPE, OBJECTIVES AND METHODOLOGY

The scope of this review was limited to decentralized department and "casual" use of third party IT services without the supervision of UCSB IT departments.

Our audit objectives included determining whether:

- There are appropriate use guidelines and procedures in place.
- Contractual arrangements are in place to protect the university's interests and to comply with laws, regulations, and UC policies.
- There is adequate provision for the ownership, protection, and retention of data.

To accomplish our objectives, our detailed work included interviews, direct observations, review of documentation, and other steps:

- Review of UC policies related to electronic communications, information security, and IT service acquisition, including:
    - UC *Electronic Communications Policy*
    - BFB IS-3, *Electronic Information Security* (Policy IS-3)
    - BFB IS-10, *Systems Development and Maintenance Standards* (Policy IS-10)
    - BFB RMP-1, *University Records Management Program* (Policy RMP-1)
    - BFB RMP-2, *Records Retention and Disposition: Principles, Processes, and Guidelines* (Policy RMP-2)
- Interviews with key campus IT personnel to more fully develop the risk areas that should be considered for coverage.
- Evaluation of the risks considered most important for the campus.
- Research and documentation of control measures that could mitigate these risks, based on IT standards, research of best practices followed by other UC campuses and other institutions, and other steps considered necessary.
- Evaluation of the extent to which control measures and best practices are in place at UCSB, and development of recommendations for improved practices to mitigate critical risks.

The Appendix to this report summarizes our evaluation of risks in this area.

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*

BACKGROUND

Third party IT services are outsourced IT services using infrastructure and applications owned, managed, and operated by third parties. Third party IT services use three basic service models:

- Infrastructure as a Service (IaaS) - Capability to provide processing, storage, networks, and other fundamental computing resources that offer the customer the ability to deploy and run software, which can include operating systems and applications (e.g., Dropbox, Amazon EC2, and Enomaly Elastic Computing Infrastructure).

- Platform as a Service (Paas) - The provider supplies a platform of software environments and application programming interfaces that can be utilized in developing new applications (e.g., Amazon Web Services).

- Software as a Service (SaaS) - Applications built and deployed for distributed computing on the Internet (e.g., Google Apps such as Google Docs and Gmail).

Benefits and Risks

There is an increase in the use of third party IT services, ranging from commonly used file hosting services to cloud-based business solutions, because they provide the following advantages:

- Cost containment.
- Immediate provisioning of resources.
- Ability to adjust resources according to demand, with little notice.
- Ability of the customer to focus on core competencies instead of devoting resources to IT operations.
- Mirrored or backup solutions to minimize the risk of downtime.

However, the use of third party IT services can increase risks to the campus in several ways[1]:

- Greater dependency on outside resources:
    - Increased vulnerabilities in external interfaces.
    - Increased risks due to use of multiple data centers.
    - Lack of robust security.
    - More difficult to perform independent assurance reviews.

- Increased complexity of compliance with laws and regulations:
    - Greater privacy risks.
    - Trans border flow of personally identifiable information.
    - Legal issues (liability, ownership, etc.) due to differing laws in host countries that may put data at risk.
    - Contractual compliance.

[1] See Appendix for Summary of Risk Evaluation.

- Reliance on the Internet as the primary conduit to the organization's data introduces:
    - Security issues with a public environment.
    - Internet connectivity and availability issues.
- Due to the dynamic nature of these services:
    - The location of the hosting or processing facility may change, which can introduce unanticipated, and unplanned for, compliance and other risks.
    - The sharing of operating facilities with some other organizations may be inconsistent with UC standards and policies.

The extent of the current use of third party IT services by the campus is not easily assessed, because of the ease with which these services can be obtained without the involvement of Procurement Services and IT departments and groups. The services are free in many cases, or they can be paid with FlexCard[2], which requires limited involvement of Procurement Services. In addition, technical and IT expertise is usually not required to use the services.

In addition, effective oversight and management of the use of these services is limited due to:

- A decentralized campus IT environment that limits the:
    - Implementation and enforcement of common standards and practices.
    - Provision of centrally-provided resources as alternatives to third party services needed or requested by the campus community.
- Incomplete IT services inventories; IT departments generally only have control and oversight over the services that they provide, and this information is not systematically shared between departments.
- The inability of IT departments to effectively control the casual use of third party IT services that do not require local installation or (as noted) technical and IT expertise.

Global Agreements

The University of California Information Technology Leadership Council (ITLC) has been working to develop technical agreements with Amazon Web Services. We also noted that University of California Office of the President (UCOP) has generated strategic agreements with a limited group of cloud service providers. Global agreements could reduce the acquisition cost of these services, and reduce risks by introducing and standardizing adequate contractual safeguards.

[2] A UCSB campus procurement card program.

SUMMARY OPINION

The result of our work indicate that existing policies, procedures, and guidelines are not sufficient to help ensure the protection of University data and compliance with laws, regulations, and UC policies. There is a need for the campus to address the risks associated with the use of third party IT services by developing, vetting, and issuing a campus policy covering the purchase and use of third party IT services, along with more detailed procedural and other guidance. There are also immediate opportunities to promote campus best practices and to mitigate risks in advance of the development and approval of campus policies and procedures, including web-based guidance and educational efforts to help the campus community to understand the risks of these services, and best practices to reduce those risks. We noted that some UC campuses have implemented and communicated relevant guidelines to their campus communities.

Audit observations and management corrective actions are detailed in the remainder of the audit report.

DETAILED OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

Table 1 Comparison of Contractual Protections

Clause	Box.com	Dropbox for Business	Dropbox
Data Privacy (FERPA)	✓	✗	✗
Data Privacy (HIPPA)	✗	✗	✗
Liability	✓	$ 100,000	$20
Campus Ownership	✓	✓	✗
Data Retention (Days)	90 after Expiration	✗	✗
Data Integrity	✓	✓	✗
Trans Border Protections	✓	✗	✗
Audit Report (SSAE 16)	✓	✗	✗
Background Checks for Provider Employees	✓	✗	✗
Communication of Security Breaches (Days)	45	✗	✗
Advance Notice of Termination (Days)	Expiration	30	0
Service Level Agreements	✓	✗	✗
Copyright Disclaimer	✓	✓	✓
Communication of Modification of Terms (Days)	60	30	✗
Permanent Deletion of Files	✓	✗	✗

Source: Auditor Analysis. The information from Box.com was obtained from an agreement between The Regents of the University of California and Internet2 to provide Box.com services at UC Davis. The information for Dropbox was obtained from the privacy policy and terms of service published by Dropbox.
✓ Provision included.
✗ Provision was not included or was not considered adequate.

A. Address Risks with Campus Policies, Procedures, and Guidelines

There is a need for the campus to address the risks associated with the use of third party IT services by developing, vetting, and issuing a campus policy covering the purchase and use of third party IT services, along with more detailed procedural and other guidance. Our review of existing policies, procedures, and guidelines found that existing guidance in related areas is not sufficient. For example:

- Policy IS-3 requires the protection of university data and compliance with federal and state laws and university policies for privacy and security, as well as outlining basic standards for contracts with third party providers.[3] However, Policy IS-3 and other existing guidance do not specify procedures, detailed guidelines, or standard, required contract provisions relating to information security in the context of the purchase and use of third party IT services.

[3] In addition, Appendix DS, a required appendix for certain types of contracts, includes contractual provisions related to restricted information that UC contractors need to comply with. However, the scope of this requirement does not include other non-restricted types of information that should be protected, such as research data.

- Policy IS-10 does not provide a complete framework for the acquisition of third party IT services in the context of systems development. For example, the policy does not provide guidance on standard, required provisions for contracts with external IT service providers that may be needed to protect the University and its stakeholders.

- The UC *Electronic Communications Policy* requires that campuses provide users with information regarding copyright laws and refer them to the university's guidelines for compliance with the online service provider provisions of the Digital Millennium Copyright Act.[4] The policy does not include guidelines or best practices to help ensure that copyright and other protections are built into relationships with third party IT service providers.

- Existing campus policies and procedures do not address the key areas that UC systemwide policies and guidance do not sufficiently cover. For example, there is limited to no guidance on the role of IT departments in the procurement of third party IT services, and there is no campus requirement that personnel consult with an IT department before using or purchasing third party IT services. It is not uncommon in other organizations for IT departments to have at least a consultant role in the IT procurement process; such a role could be particularly effective in mitigating the risks associated with the use of third party IT services, especially the casual use of these services that this audit mainly addresses.

We recommend:

- Evaluating the sufficiency of existing policies, procedures, and guidance, such as Policy IS-3 and Policy IS-10, in providing guidance for the procurement and use of third party IT services. This evaluation should be focused on identifying gaps in existing policies and procedures that campus guidance would need to cover in order to help mitigate risks in this area.

- Creating and obtaining approval for a policy and procedure(s), through the campus policy and procedure review and approval process, that address the procurement and use of third party IT services. This guidance should be specific as to:

    - The roles and responsibilities of central IT departments, campus departments and their IT units, and individual purchasers and users.
    - Required contractual protections in areas such as data privacy, liability, ownership of data, and other areas addressed later in this report.
    - The use of approved alternatives to the casual use of third party services.

[4] The Digital Millennium Copyright Act criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.

B. Promoting Best Practices

There are immediate opportunities to promote campus best practices and to mitigate risks in advance of the development and approval of campus policies and procedures. These opportunities include web-based guidance and educational efforts to help the campus community understand both the risks of these services, and best practices to reduce those risks. Specific subject areas that could be covered include:

- *Procurement* - As discussed in the Background section of this report, a significant percentage of third party IT services are free or can be obtained with minimal participation by Procurement Services and IT departments. IT service vendors can therefore provide their services without appropriate contractual protections and without the compliance requirements of UC policies. Typical "click-through" agreements offer little in the way of contractual protections:

    - Vendors do not accept any responsibility or very limited responsibility related to confidentiality, integrity, or availability of any data uploaded to their services. This is a particularly noteworthy risk because of the critical compliance requirements the University must meet, including HIPPA, FERPA, and export control regulations, among others.
    - Vendors typically only recognize data ownership by the user-owner of the account, even though university data is involved. Some vendors require free access and use of the data uploaded in these services.
    - Vendors typically do not have to communicate security breaches.
    - The agreements are subject to the laws of the country or state where these external providers are located.

- *Use of Services* - In addition to guidance on procurement, campus users should be provided guidance on the use of third party IT services. This guidance should cover areas such as agreements that individuals may not accept or sign under existing UC and UCSB policies and procedures, prohibitions on the use of certain services for HIPPA-protected and other sensitive data, and the availability of preferred alternatives, such as providers with University contracts.

File sharing and storage solutions are perhaps the most common type of third party IT services used by individual users. Table 1 compares three agreements for file storage services, two standard Dropbox agreements and an agreement between Box.com/Internet2 and UC Davis. Additional details regarding best practices promoted at other UC campuses are included in the Summary of Risk Evaluation in the Appendix to this report.

Web guidance and educational efforts to educate the campus on risks, and that promote the use of University agreements to meet user needs, would help the campus mitigate risks while formalized policies and procedures and other solutions are being put in place.

Management Corrective Actions

ETS agrees that the risks outlined in the report need to be addressed. This will require educating the campus community on the use of third party IT services and enhancing UCSB policies and procedures.

In conjunction with addressing the broader issue of information management, we will work with the support of the Executive Vice Chancellor, campus stakeholders, and the IT Council in to develop a long term solution that addresses the risks. This work will include:

- Guidance and Awareness: We will develop and communicate guidelines based on best practices, and provide guidance to the campus community on the use of third party IT services. Although this is by nature a continuous process, we will make measurable progress by the end of 2014.

- Policy Framework: We will collaborate with campus stakeholders in developing and promulgating a policy that includes coverage of the procurement and use of third party IT services. The broad participation of campus stakeholders and definition of roles and responsibilities will be necessary to help ensure the successful implementation of the policy. We plan to complete this by June 30, 2015.

Audit and Advisory Services will follow up on the status of this issue by January 31, 2015.

Appendix	Summary of Risk Evaluation					
IT Services	**Risks**	**Campus Wide Measures to Mitigate the Risks**	**UCSB State**	**Other UC Campuses**	**Other[1] Institutions**	**Interviews and References**
Infrastructure as a Service (Storage and Sharing of Files) e.g.: Dropbox Google Drive Amazon Web Services Carbonite Backup Apple iCloud **Platform as a Service** e.g.: Amazon Web Services **Software as a Service** e.g.: Google App Microsoft Office 365	• Organization and/or Communication Between Departments o Loss of Control and Transparency o Incomplete IT Services Inventory o Limited Resources to Offer Internal Services as Alternative for Campus Data • Policies, Procedures, and/or Guidelines o Lack of Guidance Selecting IT Service Providers ▪ Data Classification, Retention and Disposition ▪ Risk Assessment Approach o Lack of Guidance Using Third Party IT Services with Confidential and University Data • Contractual Protections o Click-Through Agreements (Potentially Expose the University) o Data Liability o Data Ownership o Service Level Agreements (Availability) ▪ Data Retention & Disposition Requirements o Data Security (Confidentiality) ▪ Internet Communications ▪ Security Breaches ▪ Access Control • Contractual Liability Selling IT Services[2] • Compliance with Laws and Regulation o Trans Border Flow of Data o Export Control Compliance o Legal Issues • Copyright & Licensing • Other Undefined Risks	• IT Governance Framework	Partial or Departmental	-	-	• **Alan Moses**, Assistant Dean for Academic Technology, College of Letters and Science • **Ben Price**, Director, Information Systems & Technology, Housing - Information Systems • **Bruce Miller**, Associate Director of Technology, ETS • **Doug Drury**, Director Business Relationship Management, ETS • **Jacob Godfrey**, Associate Director and Material Manager, Business & Financial Services • **Jim Woods**, Director of Computing, MSI • **Matthew Dunham**, Associate Director Identity & Cloud Services, ETS • **May Chang**, Associate University Librarian, Information Technology & Digital Initiatives • **Mike Tornquist**, HR Information Systems Manager, Human Resources • **Richard Kip**, Assistant Director ECI, Engineering College
		• Inventory of IT Services	Partial or Departmental	-	-	
		• Policies and Procedures	Partial[3] or Departmental	-	-	
		• Use Guidelines	None	Yes	Yes	
		• Training, Guidelines and Communication	None	Yes	Yes	
		• Data Classification	None	Yes	Yes	
		• Risk Assessment Approach (Banned Providers)	None	-	-	
		• Global Agreements, Contractual Protections and Service Level Agreements	None	Yes[4]	Yes	
		• IT Departments Involved in IT Service Procurement	Partial or Departmental	-	-	
		• Security Requirements/ Data Transfer Encrypted and Robust Access Control	None	-	-	
		• Data Retention (Backup of University Data)	None	-	-	
		• Internal Alternatives for Sensitive Data	Partial or Departmental	Yes[5]	Yes	

[1] Stanford School of Medicine
[2] iTunes apps
[3] UCOP policies
[4] UCOP (Google App and Microsoft Office 365), UC Davis (Box.com), UCLA (Box.com) , UC Merced (Box.com), UC Berkeley (Box.com), and UC San Francisco (Box.com)
[5] UCLA (IDRE Cloud Archival Storage Service)