Report on Institutional Use of Cloud Computing #14-204

We have completed our review of the institutional use of cloud computing. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

BACKGROUND

Definition
The most commonly accepted definition for cloud computing comes from the National Institute of Standards and Technology (NIST), who defines cloud computing as:

“A model for enabling 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 implemented with minimal management effort or service provider interaction.”

Simply stated, cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or personal computer.

History
In 1999, Salesforce.com became one of the pioneers in cloud computing by delivering enterprise applications via a simple website. The applications could be accessed by any customer with Internet access and companies were able to purchase the service on a cost-effective on-demand basis.

In 2002, Amazon introduced Amazon Web Services, which gave users the ability to access storage, computing solutions, and other applications through the Internet. In 2006, Amazon introduced Elastic Compute Cloud (EC2), which allowed developers to rent space on their computers to store and run their own applications.

By 2009, other companies like Microsoft and Google began delivering applications to the consumers as well as businesses in the form of simple, accessible services. Today, some institutions have deployed their own private or hybrid clouds, rather than rely on public clouds offered by third parties, which allows institutions to maintain more control over their data. By the end of 2015, it is estimated that spending on cloud computing services could be more than $180 billion. More than 60% of businesses are currently utilizing cloud computing for performing IT-related operations.
Benefits
Cloud computing offers significant computing capabilities and economies of scale that might otherwise require substantial investments in IT resources. Institutions can lower capital costs by using large-scale computing resources and adding or removing capacity to meet fluctuating service demands, while only paying for actual capacity used. Cloud computing provides quick access to computing services without additional hardware, software, maintenance or space, which, depending on the complexity, could potentially lower IT operating costs.

Risks
The use of cloud computing involves the very same risks found in the traditional IT world; however, they may be increased due to the lack of physical visibility and the perceived loss of control over assets and information. Some of these risks include data security, privacy, access, availability, ownership, and monitoring. Internal authorization of cloud computing services is also essential in reducing the associated risks.

Service Delivery Models
Cloud computing is typically implemented in three service delivery models:

Software - applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. An example would be the Fusion Talent Management application (Fusion), which is hosted on Oracle’s servers.

Storage - equipment owned by a third party is used for storage and/or backup of files and data. An example would be Box used by SBMI.

Computing - equipment owned by a third party is used for the execution of a computer program. An example would be the rental of Amazon Web Services for computational power needed as part of a large research study.

Deployment Models
The three service delivery models are offered to cloud customers in four deployment models:

Public - Made available to the general public regardless of affiliation. All users share the same resources.

Community - Infrastructure is provisioned for use by organizations with similar interests.

Private - Services and resources are supplied by and/or to only a select group like a private company, University, etc.
Hybrid – Using a public cloud provider to build a private cloud. This may include connections from cloud resources to the local or other remote resources.

Users
Cloud services are used by both consumers and businesses, as defined below:

Consumer Cloud – Allows consumers to access storage or software remotely from a device via the internet. The consumer agrees to terms of service online and usage is typically free up to a certain level. Payment, if required, is made via personal credit card. Examples include Dropbox and Google Drive.

Business Cloud – Service level agreements are formalized and installations can be more customized. Billing is more static and not based upon usage. Typically purchased via traditional contracts and payment methods. Examples include UTH-Secure Share and Google Apps for Education (UTH-Share).

Assurance & Standards
Both consumer and business clouds face a multitude of requirements and standards such as PCI, the US Sarbanes-Oxley Act, privacy protections laws, and ISO certification. With the rapidly changing environment and the number of cloud computing options, the Information Systems Audit and Control Association (ISACA) has stated that there is still a need for a suitable assurance framework that broadly meets the needs of every type of Cloud Service Provider (CSP) and client. The existing assurance frameworks can be classified into two broad categories:

1. Existing widely accepted frameworks customizable for the cloud (i.e., COBIT, ISO 2700x)
2. Frameworks built for the cloud (i.e., CSA Security Matrix, Jericho Forum Self-Assessment Scheme).

While UTHealth does not currently have a cloud computing policy or related procedures, ITPOL-029 Data Classification Policy does address minimum protection requirements to reduce the risk of a high risk data (PHI, confidential information, etc.) loss:
- Provide protection from unauthorized access, disclosure, modification, theft, and data loss
- Risk assessment (performed annually)
- Strong password requirements
- Logging and monitoring
- Access control and monitoring
- Incident handling-breaches/unauthorized access/use or abuse
- Test backups/DR plans/contingency plans
- Change management
- Data encryption when applicable

Cloud Computing at UTHealth
Recently, UTHealth implemented two local solutions for data sharing and collaboration: Novell Filr (“UTH-Secure Share”) and Google Apps for Education (“UTH-Share”). UTH-Secure Share is approved for HIPAA data, while UTH-Share is approved for all data classifications excluding HIPAA data. Family Educational Rights and Privacy Act (FERPA) data may be stored and shared in either UTH-Secure Share or UTH-Share.
OBJECTIVES

The objective of this audit was to provide management with an understanding of the use and risks associated with cloud computing at UTHealth.

SCOPE AND METHODOLOGY

Through a review of authoritative information on cloud computing, interviews with users and IT personnel, and a review of contracts and other agreements, Auditing and Advisory Services (A&AS) performed an audit of the current institutional uses of cloud computing.

AUDIT RESULTS

Cloud Computing Risks

Risks associated with consumer and business cloud products are similar, though the severity of the risk varies greatly depending on the cloud services model. Controls in the UTHealth environment focus on the business cloud uses and few controls are in place governing the types of data uploaded to consumer cloud sites. Data shared in one of the business clouds (UTH-Secure Share) resides on internal servers and is protected by firewalls, access controls, and other information security protocols. A&AS ranked the risks for the consumer cloud and the business cloud separately.

<table>
<thead>
<tr>
<th>Top Cloud Computing Risks</th>
<th>Risk Type</th>
<th>Consumer Cloud</th>
<th>Business Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>An independent third-party assessment of the CSP to assess control procedures may not be conducted or reviewed by UTHealth.</td>
<td>Security</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Data stored in the cloud could be lost, stolen, or improperly accessed.</td>
<td>Security</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Data stored in the cloud could be stored in unsafe locations or countries.</td>
<td>Security</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>UTHealth may not be aware of sensitive/proprietary information stored or shared without proper controls.</td>
<td>Security</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Password complexity and expiration controls may not be enforced through cloud applications.</td>
<td>Security</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Data may stay with the CSP after the agreement expires or an employee has been terminated.</td>
<td>Ownership</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Access to cloud applications may not be properly granted or revoked.</td>
<td>Access</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>UTHealth may not have appropriate backup of cloud data.</td>
<td>Availability</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Adequate policies and procedures for using cloud services may not exist.</td>
<td>Monitoring</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Cloud services could be procured or initiated without the involvement of Procurement, IT, or ITS.</td>
<td>Authorization</td>
<td>High</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
CSPs could be utilizing downstream cloud services without the knowledge of UTHealth.

<table>
<thead>
<tr>
<th>Authorization</th>
<th>High</th>
<th>Moderate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proper agreements may not exist between UTHealth and the CSP.</td>
<td>Authorization</td>
<td>High</td>
</tr>
</tbody>
</table>

**Cloud Usage/Institutional Controls**

A&AS obtained a consumer cloud storage activity report for two months (8/7/14 – 10/7/14) during the audit period. The report indicated a total of 161 gigabytes of data was uploaded by approximately 219 users. We selected a judgmental sample of 20 users and conducted interviews to determine the reason for using the consumer cloud service, the type of data (sensitive vs. nonsensitive) stored in the cloud, whether the data is shared with anyone, and why internal solutions such as UTH-Secure Share and UTH-Share are not being utilized. Of the 20 users in our sample, four were removed due to unverifiable IP addresses or employees being on leave.

A&AS interviewed key individuals within IT and the schools in order to develop an inventory (see Appendix A) of business cloud computing services at UTHealth. We documented how each service is used, including the types of data stored in the cloud and the common users.

### Cloud Usage

<table>
<thead>
<tr>
<th>Consumer Cloud</th>
<th>Business Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Of the 16 users interviewed by A&amp;AS, approximately 88% reported uploading business information (including de-identified research data) to consumer cloud sites:</td>
<td>More than 25 areas use the business cloud for some aspect of their business function, such as:</td>
</tr>
<tr>
<td>Personal Use Only 12%</td>
<td>• Storage of research data</td>
</tr>
<tr>
<td>Personal &amp; Business Use 44%</td>
<td>• Computational power for simulation studies</td>
</tr>
<tr>
<td>Business Use Only 44%</td>
<td>• Storage of healthcare data including PHI</td>
</tr>
<tr>
<td>With the exception of photos (which are stored with prior consent/release forms), users stated that they did not store other protected health information (PHI) in consumer cloud sites. A&amp;AS did not observe</td>
<td>• Disaster recovery and backup</td>
</tr>
<tr>
<td></td>
<td>• Managing Digital IDs</td>
</tr>
<tr>
<td>A&amp;AS selected four business cloud computing services utilized by UTHealth for further testing:</td>
<td>A&amp;AS selected four business cloud computing services utilized by UTHealth for further testing:</td>
</tr>
<tr>
<td>• UTH-Secure Share (Novell Filr)</td>
<td>• UTH-Secure Share (Novell Filr)</td>
</tr>
<tr>
<td>• UTH-Share (Google Apps for Education)</td>
<td>• UTH-Share (Google Apps for Education)</td>
</tr>
<tr>
<td>• Amazon Web Services</td>
<td>• Amazon Web Services</td>
</tr>
<tr>
<td>• Box (utilized by SBMI)</td>
<td>• Box (utilized by SBMI)</td>
</tr>
<tr>
<td>For each service, we obtained a copy of the cloud services contract, inquired about any education that the data owner and users have received, and obtained and reviewed the Service Level Agreement and Business Associate Agreement, if applicable. No issues were noted.</td>
<td>For each service, we obtained a copy of the cloud services contract, inquired about any education that the data owner and users have received, and obtained and reviewed the Service Level Agreement and Business Associate Agreement, if applicable. No issues were noted.</td>
</tr>
</tbody>
</table>
any PHI stored in consumer cloud sites while performing a cursory review of each user's cloud account.

The majority of users interviewed were not familiar with UTH-Secure Share or UTH-Share and emphasized the ease of use associated with the consumer cloud sites.

Institutional Controls

<table>
<thead>
<tr>
<th>Consumer Cloud</th>
<th>Business Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTHHealth does not currently have a cloud computing policy or related procedures.</td>
<td>UTHHealth does not currently have a cloud computing policy or related procedures.</td>
</tr>
</tbody>
</table>

Access to consumer cloud sites is not restricted. Consumer cloud services are easy to sign up for and use (and free in most cases). Employees enter into agreements by accepting the online terms of service. UTHHealth has no visibility around the usage of consumer cloud services or the types of data being uploaded, and no monitoring is performed. As a result, sensitive and proprietary data could be uploaded to the consumer cloud without being detected.

The granting and revocation of cloud application access, password complexity, and expiration controls rests solely with the consumer cloud service. Files created or edited in the consumer cloud are not backed up on UTHHealth servers. Data stored in the consumer cloud is accessible by employees even after termination.

UTHealth does not currently have a cloud computing policy or related procedures. Technology purchases above $5,000 require approval by the Vice President and Chief Technology Officer, and a review by Procurement Services; however, some business cloud purchases by UTHHealth did not meet the $5k threshold and were not subject to this requirement.

There are no institutional controls to ensure that a periodic review of independent third party assessments of CSPs is performed in order to identify control deficiencies, or to prevent CSPs from utilizing downstream cloud services without approval by UTHHealth.

Recommendation 1:
We recommend that Information Technology and Information Technology Security work together to develop and implement a cloud computing policy and related procedures to address the risks and absence of controls outlined above.

Management's Response: Information Technology and Information Technology Security will work together to develop and implement a cloud computing policy and related procedures that address the risks and absence of controls as outlined in the audit report.
Recommendation 2:
We recommend Information Technology Security develop and implement monitoring procedures to prevent and/or detect the inappropriate storage of sensitive and proprietary data in consumer cloud sites.

Management's Response: We agree with the recommendation. We will research and identify practical ways to prevent and/or detect the inappropriate storage of sensitive data in the consumer cloud sites. Based on this research, we will either implement blocking solutions that prevent access to consumer cloud sites or, if blocking proves to be too disruptive and impractical, we will implement monitoring solutions to detect and respond to inappropriate storage of sensitive data in consumer cloud sites.

CONCLUSION
UTHealth employees are using consumer cloud services to store both personal and business files, increasing the risk that sensitive and proprietary data could be inappropriately stored and/or accessed. Business cloud services are being used for a wide variety of functions across the institution. Recommendations were made to develop and implement a cloud computing policy and monitoring procedures to prevent and/or detect the inappropriate storage of sensitive and proprietary data in consumer cloud sites.

We would like to thank the IT staff and managers who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

cc: Audit Committee
Dr. Michael Blackburn
Dr. Michael Blackburn
Dr. Jaijie Zhang
Dr. Jaijie Zhang
Andrew Casas
Dr. Osama Mikhail
Amar Yousif
Dr. Jair Soares
Dr. Patrick Starck
Dr. John Valenza
Dr. George Stancel
Dr. Michelle Barton

Audit Manager: Sherri Heckendorn, CPA, CISA
Auditor Assigned: Brook Syers, CPA, CIA, CFE, CISA

Issue Date: February 9, 2015