Cloud, Outsourced, and Hosted Systems (Cloud) Internal Audit Report
Project # 2017-34
October 16, 2017

Reviewed by: [Signature]
Taylor Eighmy, Ph.D.
President
Scope & Objectives:
For purposes of this audit, cloud computing and storage was defined as those services purchased and/or managed by the institution, but owned and operated by third parties. The scope included policies and procedures relating to cloud services across the institution.

1. Determine if UTSA is aware of the type of data (research, mission critical, confidential, or other sensitive data) that is being processed or stored within cloud computing services and whether the risks and costs associated with these services are being managed.

2. Assess policies and procedures in place that define and address cloud-based computing and storages services and determine the methods used to enforce these policies.

3. Determine if current third party services are being managed by primary users to ensure information confidentiality, integrity and availability per UTSA information security standards.

Conclusion:
The use of cloud services for business and academic functions is growing exponentially across the institution increasing the risk that sensitive and proprietary data could be inappropriately stored and/or accessed. UTSA’s current processes, policies and procedures are not designed to effectively address acquisition, management, governance or data security associated with the types of cloud services being used by the UTSA community.

Non-Priority Recommendations:
- Create and modify processes to acquire, account for, govern and manage an outsourced, cloud computing business model. (High)

A Priority Finding is defined as “an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.” Non-Priority Findings are ranked as High, Medium, or Low, with the level of significance based on an assessment of applicable Qualitative, Operational Control, and Quantitative risk factors and probability of a negative outcome occurring if the risk is not adequately mitigated. This audit resulted in one High observation and no Priority Findings.
Audit Results
Cloud, Outsourced, and Hosted Systems (Cloud) Internal Audit Report
Project # 2017-34

Background
The National Institute of Standards and Technology (NIST) defines cloud computing as "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."

Full-service cloud providers are capable of covering both the needs of a single user storing personal documents or music to a CIO deciding to deploy either a portion or the entire IT infrastructure of an organization in the cloud. The technical architecture that allows for this level of flexibility centers around five main design characteristics: global access, on-demand self-service, community pooling of resources, easy provisioning, and metered usage. Another important aspect of cloud computing is its utility-oriented approach. Most third-party cloud providers offer services with a "pay-as-you-go" strategy. Organizations, both large and small, are attracted to this business model because it allows for transferring expenditures from large one-time capital purchases to a monthly or yearly subscription model.

GENERAL CLOUD SERVICE MODELS & RESPONSIBILITIES
While the adoption of cloud services and resources offers many benefits, it also raises significant risks that should be considered prior to integration into existing infrastructure. Risks unique to the use of cloud services include, but are not limited to:

- Limited visibility into the third-party provider’s controls;
- Inability to ensure contractual performance levels including responsiveness and capacity;
- Mismanagement of services by the third party, leading to account hijacking, denial of service, or data breach;
- Stability of provider market and services offered; and
- Inability of the service provider to meet regulatory, legal, or contractual requirements due to financial stress.

The higher education industry has seen rapid adoption of cloud computing. The EDUCAUSE *Trend Watch 2016* report indicates that 90% of colleges and universities reported at least a minor influence of cloud computing on their IT strategy. The report further provides an estimated percentage of cloud services that institutions plan to deploy within two- and five-year spans, as shown in the following table:

<table>
<thead>
<tr>
<th>Cloud Service</th>
<th>2016</th>
<th>2018 Projected</th>
<th>2021 Projected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software-as-a-Service (SaaS)</td>
<td>20%</td>
<td>20%</td>
<td>40%</td>
</tr>
<tr>
<td>Platform-as-a-Service (PaaS)</td>
<td>20%</td>
<td>40%</td>
<td>40%</td>
</tr>
<tr>
<td>Infrastructure-as-a-Service (IaaS)</td>
<td>20%</td>
<td>40%</td>
<td>80%</td>
</tr>
<tr>
<td>Public-cloud storage for Personally Identifiable Information</td>
<td>20%</td>
<td>20%</td>
<td>60%</td>
</tr>
<tr>
<td>High-performance cloud computing</td>
<td>20%</td>
<td>20%</td>
<td>40%</td>
</tr>
</tbody>
</table>

The EDUCAUSE data above suggest that private data centers are losing appeal, and the majority of institutions are choosing to move IT operations into third-party facilities. However, the trend data do not consider the growth of cloud storage and computing once IT services are migrated into the cloud. For example, UT Austin indicated that the amount of data stored in UTBox (an approved cloud service) increased almost 400% between 2014 and 2016, from 77 to 380 terabytes. The increased acceptance by UTSA to process and store administrative, academic, and research data on third-party cloud providers was identified as a high risk and resulted in the inclusion of this audit on the Fiscal Year 2017 audit plan.
Audit Details

The audit objectives for this review were:
1. Determine if UTSA is aware of the type of data (research, mission critical, confidential, or other sensitive data) that is being processed or stored within cloud computing services and whether the risks and costs associated with these services are being managed.

2. Assess policies and procedures in place that define and address cloud-based computing and storages services and determine the methods used to enforce these policies.

3. Determine if current third party services are being managed by primary users to ensure information confidentiality, integrity and availability per UTSA information security standards.

Cloud computing business model

Over the past ten years, UTSA computing model has slowly migrated to the use of hosted and cloud computing systems. The types of cloud services used by UTSA today include but are not limited to: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Public-cloud storage of data, High-performance cloud computing, and subscriptions to online materials. Existing policies, procedures and vendor management guidelines and training are limited regarding the acquisition, use and management of 3rd party services in support of a cloud computing business model.

| Observation: | UTSA could not provide a complete listing of cloud computing resources utilized by the various departments at UTSA. The Office of Information Technology (OIT) was able to provide a list of 18 different cloud computing services they manage. By reviewing a sample of procard, accounts payable and purchasing transactions; a review of Business Impact Analysis documents; and interviews with various decentralized IT resources, an additional 97 cloud computing resources utilized by UTSA departments were identified. |

There were no comprehensive policies, procedures, or guidelines available to provide guidance to UTSA users in the acquisition, tracking, use and management of cloud computing. Limited or no guidance was available regarding the need for
Audit Results
Cloud, Outsourced, and Hosted Systems (Cloud) Internal Audit Report
Project # 2017-34

<table>
<thead>
<tr>
<th>pre-acquisition information security risk assessments, the handling of “click-to-accept” type of agreements, acquisition of low cost services, and vendor management once a signed agreement was in place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In discussions with three different department’s utilizing cloud computing, there was a limited understanding of their vendor management obligations with regards to ensuring data was secure, adequately backed up, return and destroyed on contract cancellation, and information breach incident response reporting. One contract reviewed was for purchased software to be run on UTSA servers. The actual product used was SaaS, hosted by the vendor; therefore, the contract failed to address the cloud computing obligations for either party. However, the UTSA business area had a strong working relationship with the vendor, allowing for open dialog about the system functionality and performance.</td>
</tr>
<tr>
<td>Risk Level:</td>
</tr>
<tr>
<td>Management’s Response:</td>
</tr>
<tr>
<td>Responsible Person:</td>
</tr>
</tbody>
</table>
| Implementation Date: | 1. Produce information security standard - November 2017  
2. Submit information security standard for conversion to HOP – January 2018  
3. Produce a project plan for affected parties to collaborate and synchronizing workflows on cloud computing services acquisition and management – April 2018 |
CONCLUSION

The use of cloud services for business and academic functions is growing exponentially across the institution increasing the risk that sensitive and proprietary data could be inappropriately stored and/or accessed. UTSA's current processes, policies and procedures are not designed to effectively address acquisition, management, governance or data security associated with the types of cloud services being used by the UTSA community.

Paul Tyler
Chief Audit Executive at Interim

Carol Rapps
Audit Manager, Information Systems

Jaime Fernández
Sr. Auditor

Raul Huerta
Auditor III

Aaron Sanders
Auditor III

This engagement was conducted in accordance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.