February 2nd, 2017

Mr. Marc Milstein  
Associate Vice Chancellor and Chief Information Officer  
The University of Texas System Administration  
Claudia Taylor Johnson Hall, 2nd floor  
210 West 6th St.  
Austin, TX 78701

Dear Mr. Milstein:

We have completed our audit of Cloud Computing and Storage at System Administration and across The University of Texas System. The detailed report is attached for your review. We conducted our engagement in accordance with The Institute of Internal Auditors’ *International Standards for the Professional Practice of Internal Auditing.*

We will follow up on recommendations made in this report to determine their implementation status. This process will help enhance accountability and ensure that audit recommendations are implemented in a timely manner.

We appreciate the assistance provided by all information security staff and other personnel throughout this audit.

Sincerely,

J. Michael Peppers, CPA, CIA, QIAL, CRMA  
Chief Audit Executive

cc: Mr. Phil Dendy, Chief Compliance and Risk Officer  
Ms. Helen Mohrman, Chief Information Security Officer  
Mr. Bill Taylor, Information Security Officer, UT System Administration, Common Use Infrastructure  
Dr. Jim Gary, Director, Technology Information Services, UT System Administration  
Dr. Claire Goldsmith, Chief Technology Officer, UT System Administration  
Institutional Chief Audit Executives  
Institutional Chief Information Security Officers  
Institutional Chief Information Officers
EXECUTIVE SUMMARY

“Cloud computing” is the technical term referring to the delivery of services by a third party over the Internet, rather than the information technology (IT) hardware and software owned and maintained by the organization on its premises. These third-party cloud providers typically offer subscription-based service models: Infrastructure, Platform, and Software. For the purposes of the audit, this report will focus on the general use of cloud providers by The University of Texas (UT) System and not on any specific technology or vendor.

The rapidly expanding use of cloud technologies throughout UT System presents unique opportunities as well as challenging risks. To determine whether strategies and controls are employed that would appropriately address cloud-related risks, we reviewed UT Systemwide and institutional policies and procedures related to the use of cloud technologies and gathered supplemental information from each institution using a questionnaire and follow-up interviews with each respective Chief Information Security Officer (CISO) or Chief Information Officer (CIO).

Generally, UT System and its institutions are in various stages of maturity in developing and implementing cloud management strategies. This report includes recommendations to enhance existing policies and practices related to protection of cloud data, governance of cloud use, assessment of potential cloud providers, and training of end users.

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 and three Medium-level findings, but no Priority Findings.

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.

---

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 deploying 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 UT System institutions to 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 2016 audit plan.

**AUDIT OBJECTIVES**

The objectives of the audit were to assess whether UT System institutions, including UT System Administration, have policies and procedures in place to define and address cloud-based computing and storage services, and methods to enforce these policies. We also gathered information on institutional successes and challenges related to cloud service management.

---

2 Educause Trend Watch 2016: Which IT Trends is Higher Education Responding To? Educause is a nonprofit association whose mission is to advance higher education through the use of information technology.

3 1 TB (terabyte) is roughly equal to 85 million pages in Microsoft Word.
SCOPE & METHODOLOGY
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 UT System institutions. Our audit procedures included:

- Obtaining background information to understand the best practices relating to cloud technologies;
- Assessing existing policies and procedures for coverage of cloud computing topics, based on guidance from various sources (for example, NIST and ISACA, formerly known as the Information Systems Audit and Control Association); and
- Gathering and analyzing cloud management practices and procedures for each institution through CIO/CISO questionnaires and follow-up meetings.

This audit was primarily intended to assess whether institutions across the UT System have well-defined policies in place for the management and secure use of cloud services. Additionally, while we did collect and analyze information that was self-reported by the CIOs and CISOs across UT System, we did not perform specific, detailed compliance testing against institutional cloud policies. Our audit was conducted in accordance with guidelines set forth in the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing.

AUDIT RESULTS
The use of cloud computing across UT System faces many challenges. The rapid pace of technological change requires each institution to diligently evaluate the risks, benefits, and impact of cloud services on their organizational mission. To achieve our objectives, we performed a risk assessment before selecting to review the processes and controls in three areas:

- Protection of Data and Information Practices;
- Governance, Risk, and Compliance; and
- Training and Awareness.

Protection of Data and Information Practices

The ability to detect, respond to, and recover from malicious attacks or unintentional security breaches is one of the essential elements to effective IT systems management. Traditional on-premise network-based security measures such as intrusion detection systems (IDS) may be cost prohibitive or technically infeasible to extend into public cloud environments. For example, an IDS designed to send alerts when dangerous traffic that violates specific rules or policies is detected on local networks may be completely bypassed when organizations use cloud services that are accessible over the Internet.

We noted during the audit that only one institution employed a set of comprehensive technical safeguards to prevent the use of unauthorized third-party cloud providers. Although the size and diversity of network design and differences in technology among institutions make the success of any one Systemwide solution highly unlikely, without technical controls, it may be difficult to enforce policies relating to storing and managing confidential data in public cloud services.

This finding is considered High due to the potential level of information security risk from end user storing or using confidential or sensitive institutional data in non-approved services.
Recommendation 1A: The Systemwide Information Security Office and Systemwide Information Services should facilitate collaboration among institutions to identify potential methods and tools capable of meeting cloud security policy requirements.

Management's Response:
1) Relevant vendors or experts will be asked to present at the August CISO Council/InfoSec meeting.
2) The Systemwide CISO and Systemwide CIO will work to schedule a joint CISO/CIO meeting in the fall, 2017, or include in an already scheduled meeting.

Implementation Date: December 31, 2017

Recommendation 1B: The Systemwide Information Security Office and UT System Administration Office of Technology and Information Services should identify and implement technical controls designed to safeguard the use of cloud computing and storage by UT System Administration.

Management's Response: UT System Administration Office of Technology and Information Services will assess how to accomplish the objective with products already owned and/or look at the current market products by June 2017. An action plan will be developed and funding will be sought if necessary. An implementation schedule depends upon the approach selected and a target time frame of 2018 is likely.

Implementation Date: September 30, 2018

Governance, Risk, and Compliance

All institutions surveyed noted the use of cloud-related services for business purposes, with storage currently being the most prevalent type of use. The chart below details the institutions’ self-reported service distribution.

Most institutions negotiate cloud contracts solely for their own internal use. In addition, UT System Administration has procured Systemwide licensing for the following cloud services for potential use by each institution:
- Microsoft Office365 (business applications);
- Microsoft OneDrive (approved data storage);
- Facebook at Work (collaboration);
The University of Texas System
Cloud Computing and Storage Audit
Fiscal Year 2016

- SciQuest (purchasing portal);
- MyEdu (planning and scheduling for students);
- Equifax Workforce Solutions (human capital); and
- LivingWell (employee benefits).

Institutions have the flexibility to choose cloud products that best meet their business, security, and policy requirements, and are not required by Systemwide policy to use any one vendor. At the institutional level, specific cloud vendors should be vetted and approved to ensure users are utilizing services that meet the security and policy requirements of the institution. While all institutions and System Administration noted that some type of approval process for cloud services was in place, we noted during our review that 12 of 14 institutions and System Administration did not make available to employees an approved list of cloud services. Without providing guidance on approved cloud vendors, users may unknowingly employ services that do not meet security and policy requirements.

This finding is considered Medium due to the potential level of information security risk from end users using institutional data in non-approved services.

**Recommendation 2:** The Systemwide Information Security Office should maintain and publish for employees a list of approved cloud computing and storage services available for use by institutions and System Administration.

**Management’s Response:**
1) Identifying approved IT services is an institutional responsibility as institutions may have different requirements and policies. The purchasing process within each institution helps to enforce compliance.
2) UT System Administration will list approved cloud vendors on its website.

**Implementation Date:** April 1, 2017

ISACA defines governance as: “Ensuring that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.”

For each institution to gain maximum benefit from cloud services, understanding the full scope of benefits and risks of the service is essential. Results of our survey indicated all institutions and System Administration performed security assessments, vetted business contracts for cloud services, and reviewed control assessments prior to purchasing third-party cloud services. During our follow-up meetings, many CISOs and CIOs communicated the need for additional collaboration between institutions and System Administration to share the strengths, risks, and challenges of third-party cloud vendors. Sharing information among institutions on cloud service providers already assessed by one or more institutions will also reduce duplications of effort.

This finding is considered Medium due to the potential level of information security risk from the misalignment of cloud services to business needs.

**Recommendation 3:** The Systemwide Information Security Office should create and maintain a collaborative process for sharing among institutions the key documents associated with risk.

---

assessing and approving cloud computing and storage services. Additionally, the Systemwide Information Security Office should publish the criteria used to determine whether a third-party cloud service provider is considered sanctioned.

**Management's Response:**
1) An informal process is already in place. Plans to formalize the process are in progress.
2) Evaluation criteria must be established by each institution’s ISO. Evaluation and potential acceptance of risk is the responsibility of the data owner.

**Implementation Date:** June 30, 2017

**Training and Awareness**

Educating users effectively about security awareness is a difficult task. Faculty, staff, and students need to know that cloud-based systems may not have the same security controls found in institutionally-owned systems. In other words, activities or capabilities that might have been restricted on internal systems may not be blocked in the cloud.

All institutions are required to provide compliance training to address information security and data protection. Ten out of 14 institutions and System Administration currently do not have user training that specifically addresses security policies or best practices relating to the use of third-party cloud-based services. Without targeted security training relating to the use of cloud technologies, there is an increased risk of disclosure, modification, or loss of confidential institutional data.

This finding is considered **Medium** due to the potential level of information security risk from unclear or insufficient training of end users.

**Recommendation 4:** The Systemwide Information Security Office should develop additional compliance training to inform users on the appropriate use of cloud services at System Administration.

**Management’s Response:** Training materials will be created and incorporated into compliance training by the end of FY17.

**Implementation Date:** August 31, 2017

**Lessons Learned: Successes and Challenges**

**Successes**

As with many new technologies, it is common for educational institutions to be early adopters. One of the first services UT System institutions sought to migrate to cloud services was email. Institutions realized that email, though an essential service, can be burdensome to manage. In 2013, UT System Administration purchased Systemwide licenses of Office365 to provide access to cloud versions of Microsoft Exchange (for email), SharePoint (for online collaboration), and Microsoft Office applications. Many of the institutions have migrated their centralized email servers to Office365, which allowed shifting of IT resources to other critical local projects.
Challenges

With little to no initial cost, faculty, staff, and students can easily leverage cloud applications and infrastructure to process and store institutional data outside the view of both the information security office and IT support. As a result, it becomes extremely challenging for IT (including information security) to identify and manage cloud services, and protect sensitive and confidential institutional data.

Although cloud providers design services to meet operational requirements, the technical considerations from a security architecture standpoint can present challenges. IT organizations looking to move core business applications into the cloud may force local operations to extend security policy requirements across their internal networks into the external cloud environments. Not only does extending the security zone require staff capable of managing the additional complexity, but also the potential cost of managing the security infrastructure in an external virtual environment may eliminate any savings achieved from moving to cloud services.

CONCLUSION

The UT System institutions are currently in various stages of maturity in developing and implementing cloud management strategies. Based on our review of policies and procedures, questionnaire responses, and follow-up meetings, all institutional CIOs and CISOs are aware of the emerging use of cloud computing and storage, and the related risks. Although institutions have policies in place, the strength of enforcement practices varies. We noted opportunities for improvement and recommended the Systemwide CIO and CISO assist the institutions by providing additional guidance relating to cloud policies, procedures, and training, which we believe will help reduce risks through increased user awareness and acceptance of each institution’s responsibility to protect its data, regardless of where they reside.

J. Michael Peppers, CPA, CIA, QIAL, CRMA
Chief Audit Executive

Tod Maxwell, CISA, CISSP, GSNA
IT Audit Project Manager