UTHealth™

The University of Texas
Health Science Center at Houston

Office of Auditing & Advisory Services

# 18-210 Citrix

We have completed our audit of Citrix. 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

Citrix is an application that allows users to remotely and securely connect to servers, applications, and data. A total of 13 high-risk applications are currently available through Citrix, including Allscripts, GE Centricity Business (GECB), and Sunrise Clinical Manager.

## OBJECTIVES

The objective of this audit was to determine whether controls around the Citrix application are adequate and functioning as intended.

## SCOPE PERIOD

The scope period was January 9, 2018 – January 9, 2019.

## METHODOLOGY

The following procedures were performed:

- Obtained a list of users with administrative privileges, verified appropriateness based on job titles and responsibilities, and determined whether an ongoing review of administrative access is performed. Selected a sample of users granted access during the scope period and verified appropriate access approvals were obtained. Verified Citrix is authenticated through Active Directory, two-factor authentication is enabled, and sensitive computer functions (right-click, task bar, keyboard shortcuts) are disabled for non-administrative users.
- Verified data is appropriately encrypted at rest and in transit to/from Citrix servers. Determined whether Citrix servers are rebooted on a nightly basis. Verified only whitelisted sites can be uploaded to or accessed in the Citrix environment, and verified implementation of malware protection (Trend Micro) on Citrix servers.
- Selected a sample of Citrix downtime reports during the scope period and verified issues were resolved and documented on a timely basis. Determined whether server and event logs are monitored and verified alerts are followed up on as needed. Verified Citrix is up-to-date with current patches, and formal policies and procedures for Citrix exist.

## AUDIT RESULTS

A&AS identified the following areas for improvement:

- Some Citrix servers do not have the Splunk Forwarder software installed; others have the Splunk Forwarder software installed but logs are not being transmitted to the Splunk application. Additionally, server and event logs are monitored on a manual basis; however, the response to critical event logs or unusual activity is not documented.

- There is no periodic review of users with administrative access to Citrix. Additionally, there is no periodic review of enterprise and domain administrative access to Active Directory.

**NUMBER OF PRIORITY FINDINGS REPORTED TO UT SYSTEM**
None.

We would like to thank the staff and management within the Data Center Operations and Services (DCOS) and IT Security who assisted us during our review.

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

## MAPPING TO FY 2018 RISK ASSESSMENT

| | |
|---|---|
| **Risk (Rating)** | A user inadvertently introduces malware while in the Citrix environment. (High)<br>Data leakage or breaches within the Citrix environment. (High) |

## AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

| | |
|---|---|
| **Assistant Vice President** | Daniel G. Sherman, MBA, CPA, CIA |
| **Audit Manager** | Brook Syers, CPA, CIA, CISA, CFE |
| **Auditor Assigned** | Tammy Tran Coble, CISA |
| **End of Fieldwork Date** | February 26, 2019 |
| **Issue Date** | April 9, 2019 |

**Copies to:**
Audit Committee
Richard Miller
Amar Yousif
Kevin Granhold

| | |
|---|---|
| **Issue #1** | Control AU-6 of the Control Standards Catalog (a supplement to Texas Administrative Code 202) requires the organization to review and analyze information system audit logs on a defined frequency for indications of unusual activity.<br>Section 6.2.3.3 of the *Host Configuration Policy* (ITPOL-006) states system logging must be enabled to send real-time logging data to a secured logging server owned by IT Security (i.e., Splunk).<br>A&AS noted the following:<br>• Some Citrix servers do not have the Splunk Forwarder software installed as required by ITPOL-006; DCOS management informed us they are in the process of completing installation on all Citrix servers.<br>• Some Citrix servers have the Splunk Forwarder software installed; however, the logs are not being transmitted to the Splunk application. IT Security informed us they are investigating the circumstances in order to determine the appropriate resolution.<br>• Server and event logs are currently monitored on a manual basis by DCOS; however, the response to critical event logs or unusual activity is not documented. Management informed us they are in the process of transitioning to and configuring alerts in a new product, Solar Winds, that will provide this documentation. |
| **Recommendation #1** | We recommend DCOS management:<br>• Continue to expedite efforts to complete installation of the Splunk Forwarder software on all Citrix servers.<br>• Formally document the response and review of server and event logs, including actions taken to address any critical event logs or unusual activity.<br>Additionally, we recommend IT Security management continue to investigate the circumstances around the logs not being transmitted to the Splunk application, and perform remediation as deemed necessary. |
| **Rating** | Medium |

| | |
|---|---|
| **Management Response #1a** | IT Security will work with the Citrix team to verify that Citrix system logs are transmitted to the Splunk application (verified by A&AS during fieldwork).<br>Additionally, IT Security will work to set up alerts to trigger when Citrix systems stop transmitting logs to the Splunk application. |
| **Responsible Party #1a** | Amar Yousif, Associate Vice President and Chief Information Security Officer |
| **Implementation Date #1a** | July 8, 2019 |

| | |
|---|---|
| **Management Response #1b** | The Splunk Forwarder software has been added to the Citrix servers lacking the Splunk Forwarder software (verified by A&AS during fieldwork). |

| | |
|---|---|
| | Additionally, Information Technology is implementing Solar Winds for Servers, which will maintain a record of responses to alerts as well as the review of events being logged. |
| **Responsible Party #1b** | Kevin Granhold, Executive Director and Chief Technology Officer |
| **Implementation Date #1b** | August 1, 2019 |

| | |
|---|---|
| **Issue #2** | Control AC-2 of the National Institute of Standards and Technology (NIST) Special Publication 800-53 requires the organization to review accounts for compliance with account management requirements at a defined frequency. Examples of account management requirements include additional scrutiny of users with administrative privileges.<br>Management informed us there is no periodic review of users with administrative access to Citrix. Additionally, there is no periodic review of enterprise and domain administrative access to Active Directory. |
| **Recommendation #2** | We recommend DCOS management perform and document a periodic review of users with administrative access to Citrix and a periodic review of enterprise and domain administrative access to Active Directory. |
| **Rating** | Medium |
| **Management Response** | A procedure for periodic review of users with administrative access to Citrix and a periodic review of enterprise and domain administrative access to Active Directory will be implemented. |
| **Responsible Party** | Kevin Granhold, Executive Director and Chief Technology Officer |
| **Implementation Date** | August 1, 2019 |