Single Sign-on

Audit Report # 20-107
May 8, 2020

The University of Texas at El Paso

Office of Auditing and Consulting

"Committed to Service, Independence and Quality"

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU

May 8, 2020

Dr. Heather Wilson
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Wilson:

The Office of Auditing and Consulting Services has completed a limited scope audit of Single Sign-on. Based on the results of audit procedures performed, we conclude Enterprise Computing strengthened existing security controls by implementing our recommendations included in the separate management letter. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by Enterprise Computing and the Information Security Office during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:

Mr. Richard Adauto III, Chief of Staff

Ms. Guadalupe Valencia-Skanes, Interim Vice President for Information Resources

Mr. Luis Hernandez, Assistant Vice President, Enterprise Computing

Mr. Gerard Cochrane, Chief Information Security Officer

Ms. Vanessa Monzon-Cochrane, Assistant Director, Software Development, Enterprise Computing

Mr. Lethick Leon Cruz, Assistant Director, System Support, Enterprise Computing

Ms. Mary Solis, Director and Chief Compliance and Ethics Officer

University of Texas System (UT System):

System Audit Office

External:

Governor's Office of Budget, Planning and Policy

Legislative Budget Board

Internal Audit Coordinator, State Auditor's Office

Audit Committee Members:

Mr. Joe R. Saucedo

Mr. Daniel Garcia

Dr. Giorgio Gotti

Mr. Mark McGurk

Mr. Fernando Ortega

Dr. John Wiebe

Auditor Assigned to the Audit:

Victoria Morrison

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of Single Sign-on to determine adherence to State and University security controls and standards. Due to the high inherent risk of exposing functionality and/or set up of Single Sign-on to external resources, a separate management letter has been issued. These confidential results are exempt from the Texas Public Information Act under Texas Government Code §552.139.

See "Audit Results" section for a table with the issues identified during the audit.

BACKGROUND

Users usually require access to more than one application during their workday. Without a Single Sign-on (SSO) solution, users must first log into their computers and then using different credentials, log into each separate application they use. This increases the chance of users not being able to remember their passwords and/or users writing down their passwords near their workstations; increasing the risk of security breach.

With SSO, users log in (authenticate) one time via SSO and do not have to repeat the process for the duration of the session, giving the user access to multiple applications. This eliminates the need for a user having to remember multiple accounts and passwords, decreasing the risk of a security breach. Also, from a security point of view, a user's access may be enabled/disabled to multiple systems, platforms, and other resources with one set of login credentials.

UTEP has been using SSO solutions for about 15 years. About five years ago, UTEP went from an in-house developed SSO to industry standard solutions.

SSO is considered high risk due to unauthorized users being able to gain access to multiple applications with a single set of stolen credentials.

AUDIT OBJECTIVES

The objective of the audit was to ensure Single Sign-on (SSO): (i) administrative access and configuration changes are controlled and (ii) security controls around server(s) hosting SSO are in place.

SCOPE AND METHODOLOGY

The scope of the audit was limited to one SSO solution for the period of September 1, 2018 to February 26, 2020.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the authoritative guidelines of the *International Professional Practice Framework* issued by the Institute of Internal Auditors.

The criteria and standards used:

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C.§202.72 - Staff Responsibilities and 202.76 - Security Control Standards Catalog
- Texas DIR Security Control Standards Catalog Version 1.3
- UT System Policy (UTS 165) Information Resources Use and Security Standards
- UTEP Information Resources Use and Security Standards

Audit procedures included:

- interviewing and requesting information from key personnel,
- reviewing applicable laws, regulations, policies and procedures,
- verifying the existence of appropriate department/college policies and procedures,
- performing an IT assessment of controls, and
- limited testing where appropriate.

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority – 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.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

AUDIT RESULTS

Security Controls and Standards	Number of Observations
Access Management Controls	1
Change/Configuration Management	0
Server(s) Security Controls and Safeguards	2

* Due to the confidential nature of the audit, we issued a separate management letter to Enterprise Computing which details specific observations and recommendations. Enterprise Computing has implemented corrective actions to address these observations; these corrective measures have been validated by us.

CONCLUSION

Based on the results of audit procedures performed, we conclude Enterprise Computing strengthened existing security controls by implementing our recommendations included in the separate management letter, containing confidential results that are exempt from the Texas Public Information Act under Texas Government Code §552.139.

We appreciate the cooperation and assistance provided by Enterprise Computing and the Information Security Office during our audit.