Departmental Change in Management Audit (IT Portion)

Center for STEM Education

November 2016

The University of Texas at Austin
Office of Internal Audits
UTA 2.302
(512) 471-7117

The University of Texas at Austin
Institutional Audit Committee

Mr. William O'Hara, External Member, Chair
Dr. Gregory Fenves, President
Dr. Maurie McInnis, Executive Vice President and Provost
Ms. Patricia Ohlendorf, Vice President for Legal Affairs
Dr. Daniel Jaffe, Vice President for Research
Dr. Soncia Reagins-Lilly, Vice President for Student Affairs and Dean of Students
Mr. Darrell Bazzell, Senior Vice President and Chief Financial Officer
Ms. Mary Knight, CPA, Associate Vice President for Finance
Mr. Paul Liebman, Chief Compliance Officer, University Compliance Services
Mr. Cameron Beasley, University Information Security Officer
Ms. Christine A. Plonsky, Women's Athletics Director and Executive Senior Associate Athletics Director for External Services
Mr. Tom Carter, External Member
Ms. Susan Whittaker, External Member
Mr. Michael Vandervort, Chief Audit Executive, Office of Internal Audits
Mr. J. Michael Peppers, Chief Audit Executive, University of Texas System Audit Office

The University of Texas at Austin
Office of Internal Audits

Chief Audit Executive:	Michael Vandervort, CPA
Associate Director:	Jeff Treichel, CPA
Assistant Directors:	Angela McCarter, CIA, CRMA *Chris Taylor, CIA, CISA
Audit Manager:	Brandon Morales, CISA, CGAP
Auditor IV:	Cynthia Martin-Hajmasy, CPA Ashley Oheim, CPA
Auditor III:	Julie Drennan Bill Furman Stephanie Grayson
Auditor II:	Jason Boone Bobby Castillo Sumithra Sripatham, CPA
IT Auditor:	*Tiffany Yanagawa Mike McIntosh

* denotes project members

This report has been distributed to Internal Audit Committee members, the Legislative Budget Board, the State Auditor's Office, the Sunset Advisory Commission, the Governor's Office of Budget and Planning, and The University of Texas System Audit Office for distribution to the Audit, Compliance, and Management Review Committee of the Board of Regents.

FY16 Departmental Change in Management (IT Portion): Center for STEM Education
Project Number: 16.210

OFFICE OF INTERNAL AUDITS
THE UNIVERSITY OF TEXAS AT AUSTIN

1616 Guadalupe Street, Suite 2.302 • Austin , Texas 78701 • (512) 471-7117 • FAX (512) 471-8099

November 29, 2016

President Gregory L. Fenves
The University of Texas at Austin
Office of the President
P.O. Box T
Austin, Texas 78713

Dear President Fenves,

We have completed our audit of the Center for STEM Education. Our scope included information systems security in the Center for STEM Education.

Based on audit procedures performed, we conclude that the Center for STEM Education has complied with most of The University of Texas at Austin's security policies in the Information Resources Use and Security Policy; however, an improvement was noted regarding Backup/Recovery of Systems and Data. Our audit report provides detailed observations for the area under review. Suggestions are offered throughout the report for improvement in the existing control structure.

We appreciate the cooperation and assistance of the Center for STEM Education throughout the audit and hope that the information presented herein is beneficial.

Sincerely,

Michael W. Vandervort, CPA
Chief Audit Executive

cc: Institutional Audit Committee Members
Dr. Maurie McInnis, Executive Vice President and Provost, Office of the Executive Vice President and Provost
Mr. Carlos Martinez, Chief of Staff, Office of the President
Dr. Manuel Justiz, Dean, College of Education
Ms. Patricia Ohlendorf, Vice President for Legal Affairs
Mr. Jeff Treichel, Associate Director, Office of Internal Audits

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Conclusion

Based on the audit procedures performed, we conclude that the Center for STEM Education complies with most of The University of Texas at Austin's security policies in the Information Resources Use and Security Policy; however, an improvement in information systems security was necessary in one area. One recommendation was made to help improve information systems security controls related to Backup/Recovery of Systems and Data.

Summary of Recommendations[1]

The Office of Internal Audits identified no notable issues.

One recommendation was provided, but was considered minor in significance.

Management agrees with our observations and has provided corrective action plans which are expected to be implemented on or before March 1, 2017.

Audit Scope and Objective

The scope of this audit included information security in the Center for STEM Education. Specific audit objectives were to evaluate the adequacy and effectiveness of the Center for Stem Education's information security controls and determine compliance with relevant policies and procedures.

Background Summary

For management of IT resources, the Center for STEM Education receives IT support from one IT administrator. Additional IT support is provided by the College of Education's Information Technology Office. At the time of our audit, the center had one Linux Server, one Windows server, approximately 22 computers, and used mostly Apple operating systems. In 2015, the Center for STEM Education had zero breaches (i.e., remote attacker obtains unauthorized control of a computer), which is significantly lower than the 2015 campus-wide average of one breach per 68 computers.

[1] Each issue has been ranked according to The University of Texas System Administration Audit Issue Ranking guidelines. Please see the Appendix for ranking definitions.

BACKGROUND

According to the Center for Science, Technology, Engineering, and Mathematics (STEM) Education's website:

> The mission of the Center for STEM Education is to improve the teaching and learning of Science, Technology, Engineering, and Mathematics (STEM) by providing support for, and fostering collaboration among, researchers interested in conducting externally-funded interdisciplinary research on STEM teaching and learning, the conditions that influence it, and innovations that can maximize it. [2]

For management of IT resources, the Center for STEM Education receives IT support from one IT administrator. Additional IT support is provided by the College of Education's Information Technology Office. At the time of our audit, the center had one Linux Server, one Windows server, approximately 22 computers, and used mostly Apple operating systems. In 2015, the Center for STEM Education had zero breaches (i.e., remote attacker obtains unauthorized control of a computer), which is significantly lower than the 2015 campus-wide average of one breach per 68 computers.

SCOPE, OBJECTIVES, AND PROCEDURES

The scope of this audit included information systems security in the Center for STEM Education. Specific audit objectives were to evaluate the adequacy and effectiveness of the Center for STEM Education's information security controls and determine compliance with relevant policies and procedures.

To achieve these objectives, The Office of Internal Audits (Internal Audits):

- Reviewed the Information Technology section of the departmental questionnaire;
- Reviewed departmental information in The University of Texas at Austin's (UT Austin) Information Security Office Risk Assessment (ISORA)[3] tool and the UT Ready Disaster Recovery Plan (DRP)[4] application;
- Interviewed IT personnel; and
- Conducted testing on a sample of workstations in the department.

This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and with *Government Auditing Standards.*

[2] Center for STEM Education website: http://stemcenter.utexas.edu/about/
[3] ISORA is an annual, university-wide risk assessment of the university's information resources. https://isora.security.utexas.edu/
[4] UT Ready is a repository for units on campus to edit and maintain current plans for disaster recovery. https://utexas.kuali.co/ready/plans

AUDIT RESULTS

During Departmental Change in Management audits (IT portion), we review 15 areas in information systems security.

The following areas were applicable to the Center for STEM Education:

- Account Management;
- Administrative/Special Access;
- Management of Confidential Digital Data;
- Secure Configuration of Computers;
- Encryption and Remote Access;
- Secure Application Development;
- 3rd Party Vendors; and
- Network-based Storage;
- Backup/Recovery of Systems and Data;
- Incident Handling;
- Training;
- Information Systems Inventory; and
- Central Management of Computers.

The following areas were not applicable to the Center for STEM Education:

- Physical Access (Servers);
- E-Mail Servers.

Internal Audits noted a deficiency in one area as detailed in the remainder of this report. The issue has been ranked according to The University of Texas System Administration Audit Issue Ranking guidelines. Please see the Appendix for ranking definitions.

Backup/Recovery of Systems and Data – Disaster Recovery Plan
Audit Issue Ranking: Medium
The Center for STEM Education does not have a documented disaster recovery plan (DRP). Disaster recovery has not yet been addressed in the center. Without a documented DRP in place, the Center for STEM Education may not be able to adequately recover critical systems and data in the event of a disaster.

Section 6.2 of UT Austin's *Information Resources Use and Security Policy* states:

> Owners of Mission Critical Information Resources and of Information Resources containing Confidential Data must adopt a disaster recovery plan commensurate with the Risk and value of the Information Resource and a completed Business Impact Analysis. The disaster recovery plan must incorporate Procedures for:
>
> - Recovering Data and applications in the case of events that deny access to Information Resources for an extended period (e.g., natural disasters, terrorism);

- Assigning operational responsibility for recovery tasks and communicating step-by-step implementation instructions;
- Testing the disaster recovery plan and Procedures every two years at minimum (example: tabletop or scenario testing, leveraging major scheduled upgrades, activating actual service outages in a controlled scenario); and
- Making the disaster recovery plan available to the U. T. Austin Chief Information Security Officer and other stakeholders via the UT Ready disaster recovery planning service.

Recommendation: The Center for STEM Education management should ensure that a comprehensive documented DRP exists within UT Austin's UT Ready DRP application for all critical information resources and that it is tested at a management defined interval based upon the criticality of the service, a minimum of every two years. Additionally, the DRP should be kept up-to-date as staff and/or systems change.

Management's Response and Corrective Action Plan: STEM Management will work with the College of Education's ITO personnel to develop and implement a disaster recovery plan.

Responsible Person: Assistant Director, Teacher Education Research and Center Development
Planned Implementation Date: 3/1/2017

Post Audit Review: Internal Audits will perform follow-up work during the third quarter of FY17.

C O N C L U S I O N

Based on the audit procedures performed, we conclude that the Center for STEM Education complies with most of The University of Texas at Austin's security policies in the Information Resources Use and Security Policy; however, an improvement in information systems security was necessary in one area. One recommendation was made to help improve information systems security controls related to Backup/Recovery of Systems and Data.

In accordance with directives from The University of Texas System Board of Regents, the Office of Internal Audits will perform follow-up procedures to confirm that audit recommendations have been implemented.

A P P E N D I X

Audit Issue Ranking

Audit issues are ranked according to the following definitions, consistent with UT System Audit Office guidance. These determinations are based on overall risk to UT System, UT Austin, and/or the individual college/school/unit if the issues are left uncorrected. These audit issues and rankings are reported to UT System directly.

- ***Priority*** – A Priority Issue is an issue that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Austin or the UT System as a whole.
- ***High*** – An issue that is considered to have a medium to high probability of adverse effects to UT Austin either as a whole or to a significant college/school/unit level.
- ***Medium*** – An issue that is considered to have a low to medium probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.
- ***Low –*** An issue that is considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level. Issues with a ranking of "Low" are reported verbally to the unit and are not included in the final report.