TAC 202 Requirements 2017

Audit Report # 17-16
September 6, 2017

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

"Committed to Service, Independence and Quality"
September 6, 2017

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

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited scope audit of 17-16 TAC 202 TX DIR Requirements 2017. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. 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 greatly appreciate the cooperation and assistance provided by the Information Security Office staff during our audit.

Sincerely,

Lori Wertz  
Chief Audit Executive
Report Distribution:

University of Texas at El Paso:
Mr. Richard Adauto III, Executive Vice President
Ms. Sandra Vasquez, Assistant Vice President for Equal Opportunity (EO) and Compliance
Dr. Stephen Riter, Vice President for Information Resources and Planning
Mr. Gerard Cochrane Jr., Chief Information Security 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
Sunset Advisory Commission

Audit Committee Members:
Mr. David Lindau
Mr. Steele Jones
Mr. Fernando Ortega
Dr. Carol Parker
Mr. Benjamin Gonzalez
Dr. Gary Edens
Dr. Roberto Osegueda

Auditors Assigned to the Audit:
Ms. Victoria Morrison, IT Auditor
Ms. Monica Escandon, Internal Auditor
TABLE OF CONTENTS

EXECUTIVE SUMMARY ................................................................. 1
BACKGROUND .................................................................................. 2
AUDIT OBJECTIVES .......................................................................... 2
SCOPE AND METHODOLOGY ......................................................... 2
RANKING CRITERIA ........................................................................... 3
AUDIT RESULTS ................................................................................ 4
   Physical Environment: Visitor Access Records in Data Centers ............ 4
CONCLUSION ..................................................................................... 5
APPENDIX A: CRITERIA ................................................................. 6
EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed the compliance audit of controls due to have been implemented by February 2017, as required by the Texas Department of Information Resources (DIR) for the Security Control Standards Catalog Texas Administration Code (TAC) 202 Rule 202.76 (c).

During the audit we noted the following:

- No visitor logs are being kept or reviewed for data centers as required by Texas DIR security control **PE-8 Visitor Access Records**.
- Specific results and recommendations were provided to management in a separate document which contains confidential information and is exempt from the Texas Public Information Act under Texas Government Code §552.139.

Except for the items noted above, the University is in compliance with the following information security controls without exception:

<table>
<thead>
<tr>
<th>Control Number</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI-12</td>
<td>Information Handling and Retention</td>
</tr>
<tr>
<td>AU-11</td>
<td>Audit Record Retention</td>
</tr>
<tr>
<td>MA-2</td>
<td>Controlled Maintenance</td>
</tr>
<tr>
<td>MA-4</td>
<td>Nonlocal Maintenance</td>
</tr>
<tr>
<td>MA-5</td>
<td>Maintenance Personnel</td>
</tr>
<tr>
<td>PS-5</td>
<td>Personnel Transfer</td>
</tr>
<tr>
<td>PS-6</td>
<td>Access Agreements</td>
</tr>
<tr>
<td>PS-8</td>
<td>Personnel Sanctions</td>
</tr>
<tr>
<td>AC-14</td>
<td>Permitted Actions without Identification or Authentication</td>
</tr>
<tr>
<td>AC-22</td>
<td>Publicly Accessible Content</td>
</tr>
<tr>
<td>PE-16</td>
<td>Delivery and Removal</td>
</tr>
<tr>
<td>SA-5</td>
<td>Information System Documentation</td>
</tr>
<tr>
<td>CA-5</td>
<td>Plan of Action and Milestones</td>
</tr>
<tr>
<td>CA-6</td>
<td>Security Authorization</td>
</tr>
<tr>
<td>CA-7</td>
<td>Continuous Monitoring</td>
</tr>
<tr>
<td>CA-9</td>
<td>Internal System Connections</td>
</tr>
<tr>
<td>CM-10</td>
<td>Software Usage Restrictions</td>
</tr>
<tr>
<td>PL-4</td>
<td>Rules of Behavior</td>
</tr>
<tr>
<td>AT-4</td>
<td>Security Training Records</td>
</tr>
<tr>
<td>IR-2</td>
<td>Incident Response Training</td>
</tr>
<tr>
<td>IR-7</td>
<td>Incident Response Assistance</td>
</tr>
</tbody>
</table>
BACKGROUND

The Texas Department of Information Resources (DIR) issued the Security Control Standards Catalog that outlines mandatory and minimum requirements for information security controls to be implemented by all state agencies based on the “required by” date. The Security Control Standards Catalog TAC 202.76, is found in the Texas Administration Code (TAC) Title 1, Part 10, Chapter 202, Subchapter C.

AUDIT OBJECTIVES

The objective of the audit is to determine compliance with Information Security Control Standards Catalog TAC 202.76 controls that needed to be implemented by February 2017 per the Texas DIR.

SCOPE AND METHODOLOGY

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 audit criteria includes the Texas Department of Information Resource-Security Control Standards Catalog TAC 202 Rule 202.76 (c) for the security controls with the “required by” date of February 2017.

Audit procedures included:

- interviewing and requesting information from key personnel,
- reviewing applicable laws, regulations, policies and procedures,
- verifying the existence of appropriate institutional policies and procedures, 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

Physical Environment: Visitor Access Records in Data Centers

Safeguards are in place for the data centers Enterprise Computing (EC) and Research and Academic Data Center (RADC). The following safeguards were provided by the Chief Information Security Officer:

- "Proximity card is required to access these facilities; only a limited number of individuals are afforded this elevated privilege;
- On rare occasions when visitors are required to work on a system located in the Data Center, they are physically escorted at all times by Enterprise Computing personnel;
- Security cameras are in use to monitor activities;
- Electronic logs are maintained that record access (who and when) to the data center(s);
- The Enterprise Computing Group, located in the Union West lower level, strictly controls access to its facility. Only authorized individuals may access this general facility via proximity card (additionally, not all EC personnel are authorized or able to access the Data Center); other departments or individuals are required to ring a bell and state their business in order to gain access to the lower level.

Although UTEP has implemented the safeguards listed above, auditors did not find a visitor’s log to track visitors as required for security control “PE-8 Visitor Access Records. (See Appendix A: Criteria). The ISO stated a log is not necessary since visitors are rare, always accompanied by a staff member, and a 24 hour camera monitoring is available to alert staff of suspicious activity.

Recommendation:

Provide a Visitor’s Log to record visitor access from the data centers as mandated in the Texas Rules and Standards, security control PE-8 Visitor Access Records. The logs should be included as part of the review and monitoring of entrance and access to Enterprise Computing (EC) and the Research and Academic Data Center (RADC) by the responsible party for the facility.

Level: This finding is considered LOW risk, due to the fact that safeguards are in place.
Management Response:

A visitor log will be placed at the entrance of the datacenters. Visitors will sign-in upon entry.

Responsible Party:

Gerard Cochrane, Chief Information Security Officer, Information Security Office

Implementation Date:

September 18, 2017

CONCLUSION

Based on the results of audit procedures performed, we believe that compliance with UTEP Information Security Policy will be enhanced by implementing our recommendation.

Any other Security Control due by February 2017 but not included in this report has 1) been audited within past two years or 2) will be reported on a separate report due to confidential information and is exempt from the Texas Public Information Act under Texas Government Code §552.139.

We wish to thank the management and staff of the Information Security Office for their assistance and cooperation provided throughout the audit.
APPENDIX A: CRITERIA

1. Texas Department of Information Resources (DIR). The Security Control Standard catalogs is required by the TAC 202 Rule 202.76 (c)

**PE-8 Visitor Access Records**

... CONTROL DESCRIPTION

The organization:

a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and

b. Reviews visitor access records [Assignment: organization-defined frequency].

**IMPLEMENTATION**

**STATE**

The state organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

...

2. University Texas System 165

**UTS165 Standard 16: Data Center Security.**

16.2 Safeguards. ...

(d) controlling visitor and Vendor physical access with Procedures that incorporate the following:

1. advanced scheduling, logging, and documenting of visits;

2. escorting while on premises; and ...

3. UTEP Information Security Office Standards

**Standard 16. Data Center Security > 16.2 Safeguards >**

b) managing access, badges, and or keys ...

viii. card access and visitor logs records for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being

ix. the person responsible for the Information Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access...