THE UNIVERSITY OF TEXAS-PAN AMERICAN
OFFICE OF AUDITS & CONSULTING SERVICES

Texas Administrative Code (TAC) 202

Report No. 14-13
June 19, 2014

Dr. Robert S. Nelsen, President  
The University of Texas-Pan American  
1201 W. University Drive  
Edinburg, TX  78539

Dear Dr. Nelsen,

As part of our fiscal year 2014 Audit Plan, we completed an externally required audit of the Texas Administrative Code (TAC) 202. In 1989, the Texas Legislature enacted the Information Resources Management Act Chapter 2054, Texas Government Code, which established the Texas Department of Information Resources (DIR). With this legislation, DIR received authority to coordinate and direct the use of information resources technologies by all state agencies. Under Chapter 202 of the Texas Administrative Code (TAC), DIR published nine (9) rules as security standards for institutions of higher education.

The objective of the audit was to evaluate The University of Texas-Pan American’s (UTPA) information security program for compliance with TAC 202 information security requirements. The four sections selected for testing were Security Standards Policy §202.70, Managing Security Risks §202.72, Managing Physical Security §202.73, and Security Incidents §202.76. In performing this engagement, we reviewed TAC 202 rules, reviewed the UTPA Handbook of Operating Procedures, interviewed key personnel, and obtained evidence to support our conclusions.

The University of Texas-Pan American has established an information security program with adequate policies and procedures consistent with TAC 202 requirements. Although the majority of requirements have been met, there were two requirements related to managing security risks (§202.72) and reporting of security incidents (§202.76) that were not fully implemented. The detailed report is attached for your review.

We appreciate the courtesy and cooperation received from management and staff during our audit.

Sincerely,

Eloy R. Alaniz, Jr., CPA, CIA, CISA  
Executive Director of Audits, Compliance & Consulting Services
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>1</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT OBJECTIVE</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT SCOPE AND METHODOLOGY</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT RESULTS</td>
<td>3</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>8</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

In 1989, the Texas Legislature enacted the *Information Resources Management Act Chapter 2054, Texas Government Code*, which established the Texas Department of Information Resources (DIR). With this legislation, DIR received authority to coordinate and direct the use of information resources technologies by all state agencies. Under Chapter 202 of the Texas Administrative Code (TAC), DIR published nine (9) rules as security standards for institutions of higher education.

In accordance with TAC Rule 202.71, Management and Staff Responsibilities, Subpart (e), a review of the institution’s higher education information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or his or her designated representative(s).

The University’s Office of Audits and Consulting Services conducted this review and its objective was to evaluate The University of Texas-Pan American’s (UTPA) information security program for compliance with TAC 202 information security requirements. In performing this engagement, we reviewed TAC 202 rules, reviewed the UTPA Handbook of Operating Procedures, interviewed key personnel, and obtained evidence to support our conclusions.

The University of Texas-Pan American has established an information security program with adequate policies and procedures consistent with TAC 202 requirements. Although the majority of requirements have been met, there were two requirements related to managing security risks (§202.72) and reporting of security incidents (§202.76) that were not fully implemented.
BACKGROUND

The Texas Department of Information Resources (DIR) was established by state statute in 1989 to provide oversight of information resources management. DIR is responsible for ensuring that state agencies and universities are informed of technology trends, including methods for securing information assets. DIR published rules contained in the Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202 that relate specifically to information security standards. The standards established in these rules are categorized as follows:

1. Security Standards Policy §202.70
2. Management and Staff Responsibilities §202.71
4. Managing Physical Security §202.73
5. Business Continuity Planning §202.74
6. Information Resources Security Safeguards §202.75
7. Security Incidents §202.76
9. Removal of Data from Data Processing Equipment §202.78

In FY 2012, we conducted a TAC 202 audit of UTPA’s information security program. We evaluated §202.71, §202.74, §202.75, §202.77, and §202.78. We found that a majority of the requirements were met except for one related to creation, implementation, and testing of a Business Continuity Plan. As part of this audit, we followed up on the implementation status of the recommendation to address this finding. See Appendix A for a summary of the follow-up results.

AUDIT OBJECTIVE

The objective of the audit was to evaluate UTPA’s information security program for compliance with TAC 202 information security requirements by determining whether policies and procedures were developed and implemented.

AUDIT SCOPE & METHODOLOGY

In performing this engagement:

• We reviewed Texas Administration Code 202 rules.
• We reviewed the UTPA Handbook of Operating Procedures (HOP).
• We interviewed the Chief Information Security Officer to gain an understanding of UTPA’s information security program as well as the Director of the Computer Center.
The University of Texas – Pan American  
Texas Administrative Code (TAC) 202  
Externally Required

The four sections listed below were selected for testing. We tested the most current documentation/procedures in these areas.

1. Security Standards Policy §202.70  
3. Managing Physical Security §202.73  
4. Security Incidents §202.76

Our audit was conducted in accordance with guidelines set forth in The University of Texas System’s Policy 129 and The Institute of Internal Auditor’s International Standards for the Professional Practice of Internal Auditing. The audit was conducted between the months of January through April 2014.

AUDIT RESULTS

Security Standards Policy (§202.70)

All state institutions of higher education should apply the following standards:

- Information resources residing in the various institutions of higher education of state government are strategic and vital assets belonging to the people of Texas. These assets shall be available and protected commensurate with the value of the assets. Measures shall be taken to protect these assets against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Access to state information resources shall be appropriately managed.
- All institutions of higher education are required to have an information resources security program consistent with these standards, and the institution of higher education head is responsible for the protection of information resources.
- All individuals are accountable for their actions relating to information resources. Information resources shall be used only for intended purposes as defined by the institution of higher education and consistent with applicable laws.
- Risks to information resources shall be managed. The expense of security safeguards shall be commensurate with the value of the assets being protected.
- The integrity of data, its source, its destination, and processes applied to it shall be assured. Changes to data shall be made only in an authorized manner.
- Information resources shall be available when needed. Continuity of information resources supporting critical governmental services shall be ensured in the event of a disaster or business disruption.
- Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.
- Institutions of higher education shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.
UTPA has developed policies consistent with this rule. An information resources security program was in place providing reasonable assurance that its security standards adequately safeguard information resources.

Managing Security Risks (§202.72)

A security risk management program is essential to information security and protection. One of the elements of a risk management program is the identification of risks. This section requires the following:

- A risk assessment of information resources shall be performed and documented. The risk assessment shall be updated based on the inherent risk. The inherent risk and frequency of the risk assessment will be ranked, at a minimum, as either "High," "Medium," or "Low," based on various criteria.
- A system change could cause the overall classification to move to another risk level.
- Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the institution of higher education head or his or her designated representative. The institution of higher education head or his or her designated representative(s) shall make the final risk management decisions to either accept exposures or protect the data according to its value/sensitivity. The institution of higher education head or his or her designated representative(s) shall approve the security risk management plan. This information may be exempt from disclosure under §2054.077(c), Government Code.

The president designated the Chief Information Security Officer (CISO) to develop a security risk management plan. Through FY 2013, the CISO used the Information Security Awareness, Assessment, and Compliance (ISAAC) tool to perform the University's enterprise information resources risk assessment. ISAAC was an annual process that was developed by Texas A&M University and customized for University of Texas institutions. This tool was designed to assess the security posture of information systems and compliance with state security standards; however, the use of this tool was discontinued by UT System in FY 2014.

The Office of the Chief Information Security Officer provided us with independent penetration tests and stated that these replaced the enterprise information resources risk assessment. The last penetration tests were performed in August 2013. These tests assessed social engineering, and the internal and external network security. The risks identified by these tests are limited in scope focusing on the University’s network and not on enterprise wide risks.

Recommendation:

1. The Chief Information Security Officer should develop an enterprise wide information resources risk assessment and a security risk management plan that complies with Texas Administrative Code 202.72, Managing Security Risks. This assessment should be reviewed annually and presented to the president for approval.
Management’s Response:

1. This program is being reinitiated using National Institute of Standards and Technology (NIST) guidelines. The Information Security Handbook – Risk Assessment (ISH – RA) standard has been written and provided to the auditors. The process for conducting system risk assessments is under development. A vendor product (Qualys) has been selected and provisionally deployed to enable risk assessments to be conducted by the respective experts in each area.

Major system risk assessments are currently conducted via a qualitative risk assessment method examining the possibility of logical and physical manipulation of the information system.

Implementation Date:


Managing Physical Security (§202.73)

Access to restricted computing areas should be limited to authorized individuals to protect mission critical information and assets. This rule states the following: Proper management of physical security is essential to any information security program.

- The institution of higher education head or his or her designated representative(s) shall document and manage physical access to mission critical information resources facilities to ensure the protection of information resources from unlawful or unauthorized access, use, modification or destruction.
- The institution of higher education head or designated representative(s) shall review physical security measures for information resources at least annually as part of the risk assessment process.
- Information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.
- Written emergency procedures shall be developed, updated, and tested at least annually.
- Institutions of higher education will refer to the State Office of Risk Management for applicable rules and guidelines.
UTPA has implemented appropriate measures related to physical security management. The physical access to mission critical information resource facilities was adequately restricted and environmental control procedures were in place and functioning as intended.

**Security Incidents (§202.76)**

Incident handling and response is an important aspect of information security management. Security relevant events need to be logged, reported, and investigated. TAC 202.76 requires the following:

- Each institution of higher education shall assess the significance of a security incident based on the business impact on the affected resources and the current and potential technical effect of the incident, e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks. Security incidents shall be promptly reported to immediate supervisors and the institution of higher education Information Security Officer.
- If criminal action is suspected (e.g., violations of Chapter 33, Penal Code (Computer Crimes) or Chapter 33A, Penal Code (Telecommunications Crimes), the institution of higher education shall contact the appropriate law enforcement and investigative authorities immediately. Such security incidents shall be investigated and documented in a manner that restores operations promptly while meeting the legal requirements for handling of evidence.
- Depending on the criticality of the incident, it will not always be feasible to gather all the information prior to reporting. In such cases, incident response teams should continue to report information to the department as it is collected. The department shall instruct institutions of higher education as to the manner in which they shall report such information to the department. Supporting vendors or other third parties that report security incident information to an institution of higher education shall submit such reports to the institution of higher education in the form and manner specified by the department, unless otherwise directed by the institution of higher education.
- Summary reports of security-related events shall be sent to the department on a monthly basis no later than nine calendar days after the end of the month. Institutions of higher education shall submit summary security incident reports in the form and manner specified by the department. Supporting vendors or other third parties that report security incident information to an institution of higher education shall submit such reports to the institution of higher education in the form and manner specified by the department, unless otherwise directed by the institution of higher education.

UTPA established *HOP 8.9.3 Information Security Incident Handling Policy* as well as procedures for reporting incidents. Security incidents were reported through the UT System Information Security Incident Reporting Tool. Based on the documentation reviewed, we determined that security incidents were appropriately investigated and documented; however, the University did not have a process to report major security incidents to DIR.
Recommendation:

2. The Chief Information Security Officer should report incidents to the Texas Department of Information Resources. Timely reporting is required (preferably within 24 hours) for incidents that may:

- Propagate to other state systems; (emergency reporting)
- Result in criminal violations that shall be reported to law enforcement; or
- Involve the unauthorized disclosure or modification of confidential information, e.g. sensitive personal information

Management’s Response:

2. A review of this process revealed a misunderstanding of the reporting requirements. It was thought that incident reports made to UT System were rolled up to DIR through the UT System Incident Reporting tool. That misunderstanding was clarified. Process documentation will be updated and the team will be briefed on the requirements for reporting incidents directly to DIR as well as UT System.

Implementation Date:

Estimated completion June 15, 2014.

CONCLUSION

The University of Texas-Pan American has established an information security program with adequate policies and procedures consistent with TAC 202 requirements. Although the majority of requirements have been met, there were two requirements related to managing security risks (§202.72) and reporting of security incidents (§202.76) that were not fully implemented.

Isabel Benavides CIA, CGAP, CFE
Director, Audits and Consulting Services

Jose Gomez, MS
Information Systems Auditor III
APPENDIX A

FOLLOW-UP ON PRIOR AUDIT’S FINDINGS AND RECOMMENDATIONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Finding</th>
<th>Recommendation</th>
<th>Implementation Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Business Continuity Planning</strong> (§202.74)</td>
<td>The director of Environmental Health and Safety should complete, implement, test, and maintain the BCP according to TAC 202.78 (Business Continuity Planning) requirements.</td>
<td>Implemented</td>
</tr>
<tr>
<td></td>
<td>The director of Environmental Health and Safety (EHS) was appointed by the former vice president of business affairs as the responsible person to update and maintain the University wide BCP. The director gathered substantial documentation for the BCP from each division; however, the following requirements were not met:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Approval by the president or his or her designated representative</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Distribution to key personnel</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Offsite storage of BCP copies</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Business impact analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Risk assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implementation, testing, and maintenance management program</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>