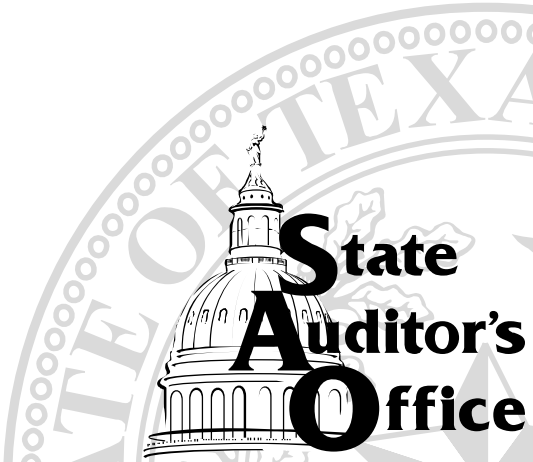
An Audit Report on

Financial System Controls at Texas Tech University

November 2005

Report No. 06-014



John Keel, CPA
State Auditor

An Audit Report on

Financial System Controls at Texas Tech University

SAO Report No. 06-014
November 2005

Overall Conclusion

Security controls over Texas Tech University's (University) financial system may not be adequate to protect critical data from unauthorized alteration or loss. Improvements should be made to the University's disaster recovery planning, physical security, user access, and internal network configuration. Conversely, the University's wireless network configuration and security are exemplary.

The University's financial system controls may not be adequate to ensure that financial data and reports are accurate, although no errors came to the auditors' attention during this audit. In addition, the University's management of those financial system controls could be improved, and inherent financial system inadequacies require continuous management intervention. The University acknowledges the financial system's inadequacies and is researching replacement options.

Background Information

Texas Tech University's (University) Financial Information Management system (TechFIM) is installed on mainframe computers located in the Technology Operations and Systems Management Data Center (Data Center) on the University's campus. The Data Center is managed by Texas Tech University System Administration (System Administration) personnel and supports functions at the University, the Texas Tech University Health Sciences Center (Health Sciences Center), and System Administration. TechFIM, which was installed in 1984, is managed jointly by the University and the Health Sciences Center.

Key Points

The University's general control environment may not adequately protect its critical data.

The University is at risk for loss of data in the event of a natural disaster or other threat because the Technology Operations and Systems Management Data Center (Data Center) does not have adequate physical protection against environmental dangers. In addition, the University's disaster recovery plans lack required components specified in Title 1, Texas Administrative Code (TAC), Chapter 202. The University's access controls also may not be sufficient to prevent unauthorized access to the mainframe computer.

The configuration of the University's wireless network is exemplary; however, the configuration of its internal network could be improved.

The University developed and actively manages a secured wireless network setup. This network is a good example of how wireless networks should be set up for university environments. The University is adequately patching and has properly configured its router-type resources. However, the patching and configuration of

State Auditor's Office
John Keel, CPA
State Auditor

This audit was conducted in accordance with Texas Government Code, Sections 321.0131 and 321.0132.

For more information regarding this report, please contact Dave Gerber, Audit Manager, or John Keel, State Auditor, at (512) 936-9500.

server resources could be improved to ensure protection of those resources from unauthorized access and compromise.

The University's financial system access controls may not be adequate to prevent unauthorized or fraudulent activity.

Employees who work in the purchasing process have excessive access, and their duties are not properly segregated. Some financial system user IDs are not specifically identifiable to individual users as required by Title 1, TAC, Chapter 202. In addition, changes to the financial system's program code are not tracked with an audit trail.

University management must continuously address and compensate for inherent financial system inadequacies.

The University's financial system has several inherent inadequacies that the University has managed through in-house development of interfacing applications and manual processes. Although the University actively monitors its financial system, some of the inherent inadequacies cause internal reporting errors and lead to decreased confidence in the accuracy of the data, which is used throughout the University. In addition, some of the manual processes that have been developed to address the financial system's inadequacies are inherently inefficient. The University recognizes the need to replace its financial system and hopes to make a decision regarding this matter by the end of December 2005.

Summary of Information Technology Review

This audit focused on the integrity and security of data in the University's financial system (the Financial Information Management system or TechFIM), as well as on the electronic purchase order module that feeds financial data to TechFIM. Auditors reviewed the management of the Data Center and also conducted network vulnerability scans and wireless leakage tests in selected areas but did not attempt to exploit the vulnerabilities identified. In addition, auditors reviewed the access and security controls for systems that authenticate users and allow general access to University networks and the financial systems.

Summary of Management's Response

The University generally agrees with the recommendations in this report.

Summary of Objectives, Scope, and Methodology

The audit objectives were to:

- Determine whether controls within the University's financial system ensure that financial data and reports are accurate.

- Determine whether security controls within the University's financial system are adequate to protect critical data from unauthorized alteration, loss, or improper use.

The audit scope included general controls over the University's information systems and application controls for the University's financial systems. The University's Office of Audit Services requested that we include the University in our planned audit of financial system controls at selected higher education institutions.

The audit methodology included interviewing staff, reviewing disaster recovery and information security plans and policies, inspecting the Data Center, conducting network and wireless scans, and reviewing security access tables to identify application control and security vulnerabilities.

Contents

Detailed Results

Appendix

Detailed Results

Chapter 1

Security Controls over the University's Financial System May Not Be Adequate to Protect Critical Data from Unauthorized Alteration or Loss

Texas Tech University's (University) management of its computer systems' general control environment (see text box) and user access controls may not protect critical data from loss or unauthorized alteration.

What Is a General Control Environment?

The phrase "general control environment" refers to the overall environment in which computer-based applications are maintained and operated. This includes not only internal security such as passwords and access rights but also physical security such as locked doors, fire-suppression systems, and off-site media storage.

The Technology Operations and Systems Management Data Center (Data Center) houses the mainframe computers on which the University's Financial Information Management system (TechFIM) and other applications essential to the University's operations reside. All of these systems contain critical information that should be protected from loss and unauthorized access or alteration. A significant loss or interruption of these systems would cause a disruption to many services the University provides.

Another critical element of the general control environment is the security and configuration of the University's network. The configuration of the University's internal network could be improved to ensure protection from unauthorized access and compromise. However, the University's wireless network configuration and security are exemplary.

Chapter 1-A

Management of the University's General Control Environment May Not Protect Critical Data in the Financial System or Other Systems from Loss

The University's general control environment is not adequately managed to protect its critical data. For example, the University is at risk for loss of data in the event of a natural disaster or other threat because the Data Center does not have adequate protection against environmental dangers. In addition, the Data Center does not provide reasonable preventive controls over unauthorized access, which leaves its equipment vulnerable to theft and loss. The University could also improve controls over access to its mainframe computer.

The University is at risk for loss of data in the event of a natural disaster or other threat because the Data Center does not provide adequate protection against environmental dangers. Specifically, auditors found the following:

- The Data Center lacks a fire-suppression system, which is essential to limit the loss of data due to a fire that affects the computer hardware or other equipment and materials located in this center.

- The Data Center lacks a backup power generator, which is essential to limit the loss of data and aid in the recovery of operations in the event of a power outage or interruption. However, the Data Center does have an uninterrupted power supply (UPS) that will provide 38 minutes of power in the event of a failure so that staff can manually power down some of the servers.

- The storage site for media on which data is backed up is located on the University campus within one mile of the Data Center. The Department of Information Resources' security policy suggests that off-site storage be in a location that is geographically different from the campus so that the backup media would not be vulnerable to the same disaster that could threaten the main site. The disasters that are most likely to occur at the University are tornadoes or severe thunderstorms; therefore, the data storage site may be too close to the main site.

The University may not be adequately prepared for a disaster that could affect its information technology resources. The University's disaster recovery plans lack required components specified in Title 1, Texas Administrative Code (TAC), Chapter 202. The Data Center's and Information Technology (IT) Division's disaster recovery plans address similar items but are separate because they pertain to two separate business functions. A review of these disaster recovery plans found that:

- The plans for the Data Center and the IT Division do not contain measures that address the impact and magnitude of loss or harm that could result from an interruption in service, as required by Title 1, TAC, Section 202.74(5)(A). An integral part of disaster recovery planning is prior identification of the significance of an event and its impact on the organization.

- The plans for the Data Center and the IT Division do not identify recovery resources (such as computers and other equipment necessary to continue operations) and a source for each item, as required by Title 1, TAC, Section 202.74(5)(B). In the event of a loss of resources, the University would have to identify sources of and negotiate agreements for alternate processing facilities, hardware, and software.

- The plans for the Data Center and the IT Division have not been tested at least annually either formally or informally, as required by Title 1, TAC, Section 202.74(5)(E). Annual testing of disaster recovery plans is critical to ensure the plans' feasibility and the preparedness of University personnel.

- The IT Division's plan does not include step-by-step instructions for implementing the plan, as required by Title 1, TAC, Section 202.74(5)(C). In the event of a disaster, users need instructions to implement the plan effectively in the midst of disaster-related confusion.

The Data Center does not provide reasonable preventive controls over unauthorized physical access, which leaves its equipment vulnerable to theft and loss. Unauthorized access could result in equipment being stolen, damaged, reconfigured, or used for unauthorized or fraudulent activities. For example, auditors found the following:

- The Data Center lacks perimeter security, such as equipment or staff to monitor the physical activity in and surrounding the Data Center. Monitoring this activity would aid in the prevention and discovery of unauthorized physical activity.

- The Data Center has one wall with oversized glass windows facing an unsecured hallway, while the other three walls are concrete. The windows are not equipped with alarms to limit the Data Center's exposure to unauthorized access.

- The Data Center's location exposes it to environmental risks. It is located on the ground floor of a renovated, multi-story building, directly beneath bathrooms and kitchenettes, creating the risk for water to leak into the center. The University reports that water has previously leaked into the Data Center.

The University's management of access controls may not be sufficient to prevent unauthorized access to the mainframe computer. Users must log in to the mainframe computer before logging in to the University's critical applications, including TechFIM. Auditors reviewed the current list of users who have access to the mainframe computer and found the following:

- The mainframe computer has 10 user accounts that are not assigned to specific individuals. This prevents the University from attributing computer activity conducted through these accounts to a specific person. The University acknowledged that these accounts were no longer needed when auditors brought them to its attention and stated that it planned to delete them.

- Two user accounts—one assigned to a previous employee and one assigned to a previous graduate student—were still enabled even though these individuals left the University in 2001 and 2002, respectively. Maintaining unnecessary enabled accounts is not compliant with University policy. In addition, Title 1, TAC, Section 202.75(3)(B), states, "A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the institution of higher education change."

- Users' passwords for accessing the mainframe are structured to be three to eight characters long and to expire every six days. Users are not allowed to reuse their last passwords; however, the mainframe keeps only one password per user in its history. This allows users to alternate between the same two passwords every six days. The Department of Information Resources recommends that passwords be at least eight alphanumeric characters, be changed at least every 60 days, and not be reused for a period of one year.

The University's programmers have direct access to production, or "live," data in the eTravel application. The eTravel application, which was developed in-house to process travel requests, interfaces with TechFIM. Because programmers have direct access to production data, they could inadvertently or intentionally manipulate data without detection, which could result in the inappropriate or fraudulent use of University resources.

The University has developed and instituted a campus-wide education program on the security of personal computers. The University asserts that the program has heightened the campus population's awareness of the necessity of security and of safe computing practices.

Recommendations

The University should:

- Install a fire-suppression system and a backup power generator in the Data Center and move its off-site data storage site farther from the Data Center.
- Update and regularly test its disaster recovery plans to comply with requirements in Title 1, TAC, Section 202.74.
- Install perimeter security at the Data Center and, where possible, modify the facility to mitigate physical inadequacies.
- Ensure that all user accounts are assigned to specific, authorized individuals.
- Require users to create passwords that are at least eight alphanumeric characters, are changed at least every 60 days, and are not reused for a period of one year.
- Limit programmer access to allow only copying of production data associated with all applications, including eTravel.

Management's Response

- *Prior to the State Audit engagement, Texas Tech began the process of securing resources to enhance the environmental aspects of the*

Technology Operations and Systems Management (TOSM) Data Center. Significant electrical upgrades have been completed. We anticipate a fire suppression system will be installed in December. We are currently working with our Physical Plant staff to size a generator to provide back-up power. Because of the long manufacturing cycle, we anticipate the generator will be installed by next July.

Currently, media containing data backed up at the TOSM Data Center is located off-site in a secure underground vault. Management believes the current process and location does not pose an unacceptable risk to Texas Tech.

- *Both the Data Center and the IT Division's disaster recovery plans went through major rewrite processes earlier this year. One of the areas remaining to be resolved is the identification of specific resources to serve as a recovery site for our mainframe operations. Texas Tech is in the process of finalizing a private sector relationship to serve as the recovery site for our mainframe operations. We expect to have this relationship finalized by December 1st. Additionally, both the Texas Tech University System and the IT Division are engaging outside resources to assist us in conducting a risk assessment/business continuity process. As a result of these activities, we expect our disaster recovery plans will be updated to address the issues raised in the audit report by March 1st.*

- *Perimeter security of the Data Center facility is monitored by the Texas Tech Police Department during their patrols. We are investigating the feasibility of adding exterior security cameras and an alarm system on the glass panel in the interior hall of this secured facility. Relocating the Data Center facility is not in our current plans.*

- *Nine of the ten unassigned mainframe computer accounts related to applications that have been moved off the mainframe platform or have been replaced. It is common practice at TOSM to archive datasets that belong to old applications in order to free up disk space. Mainframe internal security (RACF) controls access for each account to specific datasets. The datasets related to these accounts had been archived. Therefore, these nine accounts did not pose a risk. The other unassigned mainframe account related to a programmer's access to RaiderLink. This password has been assigned to a specific individual.*

  Out of all of the user accounts the audit staff reviewed, we are disappointed to find that one previous employee and one previous graduate student's account had not been deleted. However, it should be noted regarding the former employee's account that without a TECHNet password to gain access to the mainframe, the TechFIM user ID and password would not permit this individual access to the TechFIM application. The former graduate student's account access was limited to

specific statistical datasets related to her dissertation. The graduate student's account has been closed. We will continue to review and refine our account management procedures in an effort to build on the success of our current practices.

- *TOSM is currently testing the programming changes necessary to require an eight character alphanumeric password, increase the length of time a password is valid from six to sixty days, and restrict a password from being reused for one year. TOSM anticipates implementing these changes by year end.*

- *For project leaders, this type of access is necessary to make production changes or emergency fixes. The development group that manages the eTravel database is relatively small—five programmers and one web designer. Due to the number of different projects this group maintains, each programmer must have access to the database(s) they are responsible for. Since this arrangement introduces some risk, we have instituted several policies to minimize that risk. For situations where data must be modified, the project leader makes a request to the development group manager who manually logs the request. In addition, the database management system automatically logs this type of direct data access, which can be compared to the manual log for audit purposes. Other production database modifications follow an established change control procedure ending in final approval by the development group manager. With these safeguards and policies in place, we accept the inherent risk involved in allowing limited programmer access to production data.*

Chapter 1-B

The Configuration of the University's Wireless Network Is Exemplary; However, the Configuration of Its Internal Network Could Be Improved

The University developed and actively manages a secured wireless network setup. This network is a good example of how wireless networks should be set up for university environments.

The University is adequately patching and properly configuring its router-type resources. However, the patching and configuration of server resources could be improved to ensure the protection of those resources from unauthorized access and compromise. Auditors performed internal security scans of the University's network from inside the University's firewall. These scans identified a number of potential vulnerabilities, and auditors provided University management with the detailed results of these security scans for its follow up.

Recommendation

The University should analyze the security scan reports and take action on the recommendations for strengthening or eliminating identified vulnerabilities in accordance with its business needs and requirements.

Management's Response

The network scan reports have been reviewed and the appropriate server administrators in the university departments have been notified and all the findings have been addressed. The Network Security Team is performing regular vulnerability scans of the mission-critical systems, and will notify the appropriate personnel if vulnerabilities are discovered.

Controls within TechFIM, a mainframe application that was installed in 1984, may not be adequate to ensure that financial data and reports are accurate, although no errors came to the auditors' attention during this audit. In addition, the University should improve its management of user access and changes to the program code. TechFIM should be reasonably protected to ensure continued financial operations.

TechFIM is shared by all entities of the Texas Tech University System, which include the University, the Texas Tech University Health Sciences Center (Health Sciences Center), and the Texas Tech University System Administration. Although these entities use the same application, they each have the ability to use it in different ways. For example, separate security administrators at the University and the Health Sciences Center manage access to TechFIM.

TechFIM has several inherent inadequacies that the University has managed through in-house development of interfacing applications, system-generated reports, and manual reporting processes. These inadequacies require the University to frequently reconcile data to ensure its accuracy.

Chapter 2-A

The University's Management of Access Controls in TechFIM Could Be Improved

The University's management of TechFIM access controls may not be adequate to prevent unauthorized or fraudulent activity.

Employees in the purchasing process have excessive access, and their duties are not properly segregated. The University manages all purchases electronically via a Web-based application developed in-house that interfaces with TechFIM. Auditors found that employees involved in purchasing have access that is not appropriate or necessary to perform their jobs and that their duties are not properly segregated. This lack of segregation of duties leaves the University vulnerable to unauthorized use of University resources and loss of funds. Specifically:

- Sixteen Purchasing Department employees, including all six purchasers and three managers, have access to process payment vouchers in TechFIM. As a result, purchasers could potentially order and pay for unauthorized items without detection.

- Two Purchasing Department managers have access in TechFIM that allows them to create a vendor, initiate a request for a purchase, make the purchase, and initiate the payment to the vendor with no oversight or

approvals. They can also delete the transaction after the process has been completed. With this access, these managers can complete the entire purchasing cycle with no supervisory oversight, potentially resulting in unauthorized purchases.

- Nine percent of purchase orders auditors sampled were originated and approved at the departmental account manager level by the same person. Account managers are designated in each University department and have responsibility for approving expenses for a specific account. The application does not conduct a check to ensure that the originator and the person who approves the purchase order are different individuals.

- One user in another department has access to (1) enter, correct, and delete purchase, payment, and other accounting transactions and (2) all levels of approval over those transactions. Under normal circumstances, such transactions should require at least two levels of review by separate individuals, but this individual can generate and approve transactions with no supervisory oversight.

The University's management of financial system access controls may not protect critical data from unauthorized alteration. The University's management of access controls may not be sufficient to prevent unauthorized access and alteration of data. Auditors reviewed the TechFIM user access security table (which shows what each user has access to) and found the following:

- Two TechFIM user IDs are not assigned to specific individuals, which prevents the University from holding individuals accountable for their computer activity. In addition, as previously mentioned, one user ID is assigned to a former employee, which constitutes noncompliance with University policy and Title 1, TAC, Section 202.75(3)(B).

- The structure of the Health Sciences Center's user IDs allows multiple users to have the same IDs with different passwords. Because passwords are not included in temporary transaction logs, the specific identification of users who initiate transactions is not possible. Title 1, TAC, Section 202.75(3)(A), states, "Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users."

Changes to the TechFIM program code are not tracked with an audit trail. The University uses program code editors (software that programmers use to make changes) instead of a code management library (software that tracks and manages the changes made by programmers). As a result, programmers could make unauthorized code changes without detection. This situation constitutes noncompliance with Title 1, TAC, Section 202.75(5)(B), which states, "Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software, and for all

changes to automated security or access rules." The University is planning to implement a code management library that would address this problem.

Recommendations

The University should:

- Review users' access for appropriateness and limit access as necessary to properly segregate duties.
- Review and delete user IDs that are not assigned to specific, authorized users or are assigned to users who no longer require access.
- Create and implement a policy requiring all users to have unique user IDs.
- Institute policies and develop edit checks that prevent the same individual from both initiating and approving a purchase.
- Continue with the planned transition to a code management library.

Management's Response

- *At TTU, extensive work has been done during the past year to cleanup user access within TechFIM. Specific access problems identified during the audit that were excessive or prevented segregation of duties, primarily in TTU Purchasing, have been corrected.*

  TTU will continue to review access in TechFIM for appropriate access with proper segregation of duties. Policies will be modified as required.

- *This issue was previously addressed in our management response to two issues previously raised in this report.*

- *Texas Tech currently has a policy that requires users with data entry permissions to have unique user IDs. We do not believe the use of a generic user ID field to identify a department or campus at the HSC, poses a risk. This generic user ID along with a unique password only provides scan and inquiry access. Transactions can not be entered through this type of access. We believe this practice is consistent with the TAC requirement since our risk analysis demonstrates there is no need for individual accountability for inquiry access.*

- *Management does not believe this issue raises a material risk, since all transactions are ultimately approved by the appropriate purchasing group in the Purchasing Department before processing. For small departments, simply having the department manager assign the task to an employee to*

route a transaction to them for approval does not add a practical internal control feature and creates an unnecessary burden.

- *Information Systems staff began the initial analysis work on the use of Alchemist, source code management software, for TechFIM in Fall 2004 with the actual project work being done in calendar year 2005. The TechFIM system source code migration to Alchemist is on schedule and will be completed by the end of calendar year.*

Chapter 2-B

University Management Must Continuously Address and Compensate for Inherent Financial System Inadequacies

TechFIM has several inherent inadequacies that the University has managed through in-house development of interfacing applications and manual processes. Although the University actively monitors TechFIM, some of the inherent inadequacies cause internal reporting errors and lead to decreased confidence in the accuracy of the data, which is used throughout the University.

Manual error corrections in TechFIM are necessary but leave the data vulnerable to undetected alteration. Specifically, auditors found that:

Ensuring TechFIM's Data Integrity

TechFIM is a mainframe-based application written in the programming language COBOL that consists of a general ledger and reporting tables. These reporting tables are used to store summary totals from the general ledger for reporting and user viewing.

The University developed a budget application in-house to interface with TechFIM. The budget application was written in the Natural programming language. Because the programming languages are not the same, the nightly processing between the two applications results in processing errors that cause the amounts on the budget reporting tables to be out of balance with the general ledger.

To compensate, staff review automatically generated system assurance reports that check for accounts that are out of balance with corresponding ledger transactions. After the errors are identified, University personnel correct the out of balance accounts by directly accessing the budget reporting tables in TechFIM.

- The processing errors caused by the interface between the budget application and TechFIM require the University to frequently reconcile data manually between the reporting tables and the general ledger to ensure the accuracy of data (see text box). As often as five times a week, managers correct the errors identified on system assurance reports.

- To correct errors, users must make direct changes to budget reporting tables. Allowing users to make direct changes to the data tables within an application leaves the data vulnerable to unauthorized alteration. However, in this particular situation, it is necessary to allow users to correct errors and the access is limited to two people each at the University and at the Health Sciences Center.

- The number of errors corrected is not reconciled with the number of errors identified by system assurance reports to ensure that all errors identified are corrected. The only documentation of error correction consists of screen prints of tables before and after corrections are made, along with the related system assurance reports that are retained by the users who correct the errors.

TechFIM does not keep an audit trail of changes made to data within the system. TechFIM does not have the capability to trace user ID, terminal ID, time of transaction, or the identification of the individual who entered or edited a transaction. Title 1, TAC, Section 202.75(5)(B), states, "Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software, and for all changes to automated security or access rules."

TechFIM is not capable of segregating users' access to specific accounts. After a user is assigned access to certain documents or tables, the user has that same level of access for all accounts, departments, and institutions that use TechFIM. This allows users access to accounts for which they may not be responsible and should not be authorized to edit, change, or delete.

TechFIM contains other inefficiencies because of a lack of edit checks. For example, users are able to reuse journal voucher document IDs multiple times within the same fiscal year. These IDs are manually entered by the personnel processing them instead of being automatically assigned by TechFIM. TechFIM will not allow a document ID to be reused within an accounting period, but the table that records these IDs is automatically cleared at the end of each month. When TechFIM rejects a document because of a duplicate ID, the document is placed into a suspense file, and users must monitor the file and correct the rejected documents for resubmission. Reusing document IDs within the same fiscal year obscures the audit trail and creates inefficiencies when documents are rejected and must be corrected for resubmission.

The preparation of the University's financial reports is inefficient. The University's process for preparing financial reports involves staff's manual compilation of information from TechFIM reports to produce the final financial reports. Some reports are printed and the amounts are then input into an Excel spreadsheet, while other reports are exported directly to Excel. This is time-consuming and leaves the data vulnerable to intentional or accidental alteration. The University is currently implementing a financial reporting interface that will provide the capabilities to automatically generate financial reports.

University management recognizes the need to replace TechFIM. The University is in the process of replacing the student system and has begun looking at alternatives for TechFIM. It anticipates it will make a decision on this matter by the end of December 2005.

Recommendations

The University should:

- Resolve the conflict in the interface between the budget application and TechFIM to eliminate the nightly processing errors and the need to fix the errors through direct changes to the reporting tables.
- Develop a method to identify who initiates and edits transactions in TechFIM or create an alternative manual control so that it can identify users who make changes to data.
- Review users' access to TechFIM and limit their access to their respective areas of responsibility.
- Ensure that each document ID and transaction number within TechFIM is unique within each fiscal year.
- Continue the implementation of the financial reporting interface to automatically generate financial reports.

Management's Response

- *Substantial progress has been made in resolving the technical conflict between the budget application and TechFIM, however, as the auditors noted, the problem continues to exist causing periodic processing errors that must be fixed. These errors are reported on the System Assurance reports daily and are reviewed, corrected, and documented.*

  As the auditors noted in their report, the Texas Tech University System is actively reviewing a replacement for our current financial system. We anticipate reaching a decision on a potential replacement system by the end of December. A replacement system would resolve the current conflict between Budget and TechFIM systems. Based on the decision for a new system and implementation timeline, Texas Tech will determine if there is a need to bring in outside assistance to help resolve the conflict in the current systems.

- *All transactions go through the suspense file in TechFIM for processing. The suspense file does maintain the user ID and date of the last person accessing the transaction. Once a transaction is processed successfully, this type of information is not carried forward to the ledger files. However, transaction detail is transferred from the suspense file to an archive file.*

  As the auditors noted in their report, the Texas Tech University System is actively reviewing a replacement for our current financial system. We

anticipate reaching a decision on a potential replacement system by the end of December. A new system would provide the logging functionality necessary to track users and changes made to data for all transactions.

- *TechFIM access is granted separately for tables and transactions. While TechFIM does not provide the ability to control access by institution or at the account number level, all update access to the tables is limited to central administrative offices by appropriate area of responsibility. Access to transactions is also limited to the user's appropriate area of responsibility.*

  As the auditors noted in their report, the Texas Tech University System is actively reviewing a replacement for our current financial system. We anticipate reaching a decision on a potential replacement system by the end of December. The financial system being reviewed provides the ability to grant access based on roles and provides fine grain access functionality.

- *During Fiscal Year 2004, 32 duplicate IDs were used for journal vouchers. For Fiscal Year 2004, we processed 1,005,990 transaction IDs. While the number of duplicates was extremely low, we will write an edit that will eliminate any duplicate IDs being processed within a fiscal year. However, it should be noted none of the 32 duplicate IDs caused the duplication of a transaction or data corruption.*

- *Automation of Financial Reporting at TTU has made significant progress during the past year and is ongoing. New reports are being added and development will continue. Input for reports is being provided by user committees.*

  At TTUHSC, most reporting, including the preparation of the annual financial report, is significantly automated and sufficient to meet the needs of administrative and departmental users.

  As the auditors noted in their report, the Texas Tech University System is actively reviewing a replacement for our current financial system. We anticipate reaching a decision on a potential replacement system by the end of December. Reporting needs will be a part of the project plan in a new implementation.

Appendix

Objectives, Scope, and Methodology

Objectives

The audit objectives were to:

- Determine whether controls within Texas Tech University's (University) financial system ensure that financial data and reports are accurate.
- Determine whether security controls within the University's financial system are adequate to protect critical data from unauthorized alteration, loss, or improper use.

Scope

The audit scope included a review of (1) general and application controls over the University's financial system application and financial controls over the electronic purchase order application that interfaces with TechFIM for fiscal year 2005 and (2) completed purchase order transactions for fiscal year 2004. The University's Office of Audit Services requested that we include the University in our planned audit of financial system controls at selected higher education institutions.

Methodology

The audit methodology included interviewing staff, reviewing disaster recovery and information security plans and policies, inspecting the Technology Operations and Systems Management Data Center (Data Center), conducting network and wireless scans, and reviewing security access tables to identify application control and security vulnerabilities.

Information collected and reviewed included University policies and procedures applicable to user access, security, disaster recovery, and physical security.

Procedures and tests conducted included the following:

- Interviews with key staff regarding user access, security, disaster recovery, physical security, and electronic purchase orders.
- On-site walk-through of areas that store major information systems equipment.
- Network scans using Internet Security Systems' (ISS) Internet Scanner™.

- Wireless leakage testing to identify access points located around specific buildings. A directional antenna was used to pinpoint the access points to specific buildings.
- Analysis of user access to TechFIM, the mainframe, the Web-based authentication system for the network, and the Data Center.
- Analysis of processed electronic purchase orders.

Criteria used included the following:

- Title 1, Texas Administrative Code, Chapter 202 (Information Security Standards).
- Texas Department of Information Resources guidelines.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) guidance.

Project Information

The audit was conducted from July 2005 through October 2005. This audit was conducted in accordance with generally accepted government auditing standards. The following members of the State Auditor's staff performed this audit:

- Anthony W. Rose, MPA, CPA, CGFM (Project Manager)
- Bruce W. Dempsey, MBA (Team Leader)
- Shahpar Ali, CPA, JD
- Hillary Hornberger
- Ashley Jacobson
- Marlen Randy Kraemer, MBA, CISA (Information Systems Audit Team)
- Serra Tamur, MPAff, CIA, CISA (Information Systems Audit Team)
- Charles P. Dunlap, Jr., CPA (Quality Control Reviewer)
- Dave Gerber, MBA, CISA (Audit Manager)

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Tom Craddick, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas "Tommy" Williams, Member, Texas Senate
The Honorable Jim Pitts, House Appropriations Committee
The Honorable Jim Keffer, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Texas Tech University System

Mr. L. Frederick "Rick" Francis, Chairman, Board of Regents
Mr. J. Frank Miller III, Vice Chairman, Board of Regents
Mr. Larry Anders, Member, Board of Regents
Mr. C. Robert "Bob" Black, Member, Board of Regents
Mr. F. Scott Dueser, Member, Board of Regents
Mr. Mark Griffin, Member, Board of Regents
Mr. Daniel Serna, Member, Board of Regents
Ms. Windy Sitton, Member, Board of Regents
Dr. Bob L. Stafford, Member, Board of Regents
Dr. David Smith, Chancellor

Texas Tech University

Dr. Jon Whitmore, President