PROJECT SUMMARY

Information technology (IT) processes and controls in the Division of Finance at Texas A&M University provide reasonable assurance that IT resources are used efficiently and effectively and in compliance with laws, policies, regulations, and rules. The division’s IT resources and IT systems are centrally managed by the Information Technology Services department which reports directly to the Chief Financial Officer. Opportunities for improvement were noted in the areas of logical security and data backups.

The Information Technology Services department has an annual operating budget of approximately $1.6 million and 15 staff positions. The department provides the Division of Finance with computer operations, financial analysis, and application and website development.

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. Logical Security

Observation

The Division of Finance has taken several proactive steps to reduce operational security risks and has virtualized servers and automated certain processes for increased efficiencies. However, certain areas were noted in which logical security requires improvement to further strengthen the division’s IT security posture.

Logical security was reviewed for 12 Windows operating systems and 6 SQL databases. Opportunities for improvement were noted in the following areas:

- In general, no minimum password age is enforced for the Windows domains or by the individual systems' local policy. Three servers' local password policies were still using the...
Windows default settings which do not enforce generally accepted password security settings. For 4 of the 6 SQL servers (66%), passwords were able to be discovered through the audit process due to poor passwords selected by users or IT personnel. In one instance, a third-party application allowed poor passwords, because it does not have password settings that allow enforcement of University password requirements.

- IT personnel effectively login as domain administrators at all times, whether the elevated rights are required or not. It was noted that this was due in part to their transition to a new domain and would be corrected once the transition was complete.

- Passwords and personally identifiable information were found to be stored in plain text within a database due to limitations in a vendor's application, and logins were not encrypted on several websites and an FTP server. Management was not aware of unencrypted passwords and personally identifiable information issues, but has since contacted the vendor and is working to address the website and FTP issues.

Texas Administrative Code 202.70 states that "...measures shall be taken to protect these assets against unauthorized access, disclosure, modification, destruction, whether accidental or deliberate, as well as to assure asset availability, integrity, utility, authenticity, and confidentiality of information." Standard administrative procedures (SAPs) have been developed by the University to provide guidance regarding minimum IT security requirements. Failure to implement strong logical security practices increases the risk that sensitive files or systems could be compromised and critical services could be disrupted.

Recommendation

Strengthen logical security practices with the following:

- Enforce current University SAP password standards and develop, document and implement a minimum password age wherever possible. For existing accounts, including those whose associated passwords were identified as poor during the audit, require users to change their passwords to meet the new standards. Provide additional training for identified noncompliant users.

- Pre-deployment hardening for all systems and devices should be performed and include the enforcement of minimum security
criteria in compliance with University SAPs. The minimum pre-deployment security criteria should include, but are not limited to, changing default passwords and default device settings.

- For personnel with administrator/privileged access, create a separate, non-privileged account for 'normal' daily use.

- Where a vendor's application does not encrypt confidential information or does not have password controls in place, communicate this oversight to the vendor, and request that password encryption and password controls be implemented. Follow-up as necessary, and involve other interested parties if deemed appropriate (e.g., the University Information Security Officer).

- For FTP services and websites that allow logins and transmit sensitive/confidential information, obtain and install valid SSL certificates (e.g., InCommon certificates through University CIS), and force communication via SSL wherever possible or replace with more secure services.

**Management's Response**

- **Group policies have been reviewed, adjusted, re-applied, and documented to enforce current University SAP password standards.** For accounts whose associated passwords were identified as poor, the passwords will be changed to meet University SAP password standards or the account will be deleted. Additionally, IT staff has reviewed password requirements for system administration accounts and will monitor for compliance.

  *Target date: March 31, 2012.*

- **We have reviewed and modified our documented server pre-deployment procedures to be in compliance with University SAPs. IT staff will be trained to use these procedures.**

  *Target Date: April 30, 2012.*

- **For personnel with administrator/privileged access, a separate non-privileged account has been created for normal daily use. These employees use their normal (un-privileged) account for everyday use and only use the privileged account for specific system administration.**

  *Target Date: Complete.*
• For the application identified during the audit utilizing plain text storage, a written notification dated January 24, 2012 was sent to the vendor requesting that specific fields stored in the application’s database be encrypted and the application be modified to include an enforceable password policy. We will continue to follow up with the vendor until these items are completed and if needed will communicate status to the University Information Security Officer by May 31, 2012.

Target date: May, 31, 2012.

• Three legacy servers that required authentication are no longer needed and were shut down. A SSL certificate was installed on the remaining server that required user authentication. The FTP server has been configured to allow only secure FTP connections and the remaining six user accounts have been changed to use the secure FTP process.

Target Date: Complete.

2. Data Backup Testing

Observation

While three different types of data backups are being performed on a scheduled basis, they are not fully tested on a scheduled basis. Currently, the only tests performed are actual data restore requests. However, these requested recoveries do not ensure that all required operating system settings and data files could be restored if the primary data center or systems could not be accessed. Critical system backups should be periodically tested to ensure that all applications/settings/data could be restored if the primary storage media were unavailable.

TAC 202.74 requires that mission-critical information be backed up on a scheduled basis. Department of Information Resources "Practices for Protecting Information Resources" further states that backup media should be tested regularly and frequently for recovery/restorability of files. Failure to plan for and test all critical data backup practices in use increases the risk that mission-critical data will be lost or will not be available in a timely manner in the case of a disaster or other loss of service.

Recommendation

Plan and schedule tests of the data backup system to ensure that it has the capability to restore data from all backup methods. Track
the tests completed and monitor to ensure all scheduled tests are performed as intended.

Management’s Response

A schedule has been developed to perform restore tests four times a year (quarterly). Each backup method will be tested and documented during these events. As each backup method is tested, the servers and data that are restored will be changed so that over time, every server/data type will be tested. This will help insure that each backup method is tested and that numerous servers, databases, and applications are tested during each event. The first quarterly test will be completed and documented by May 31, 2012.

Target Date: May 31, 2012.

BASIS OF REVIEW

Objective and Scope

Review the processes and controls over information technology in the Division of Finance to determine if resources are used efficiently and effectively and in compliance with laws, policies, regulations and rules. The Information Technology Services department is responsible for the procurement, installation, support and security of all servers, computers, mobile devices and software applications used by the Division of Finance. The department is also responsible for specialized Division of Finance server applications such as Campus Loan Manager, AggieBuy middleware services, Payformance and Document Imaging. The audit period focused on activities from September 1, 2010 to January 26, 2012. Fieldwork was conducted from November 2011 to January 2012.

Criteria

Our audit was based upon standards as set forth in the System Policy and Regulation Manual of the Texas A&M University System; Texas Administrative Code 202, Information Security Standards; and other sound administrative practices. This audit was conducted in conformance with the Institute of Internal Auditors’ “International Standards for the Professional Practice of Internal Auditing.”
Additionally, we conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The stated mission of the Information Technology Services department is to provide computing solutions and support services to the Division of Finance and its customers at Texas A&M University. The department is responsible for the procurement, installation, support and security of all servers, computers, mobile devices and software applications used by the division. Services performed by Information Technology Services directly impacts students, parents, faculty, and staff. The department is comprised of three areas: Computer Operations; Financial Analysis and Data Reporting; and Application and Website Development.

AUDIT TEAM INFORMATION

Dick Dinan, CPA, Director
David Maggard, CPA, Audit Manager
Kim Rutledge, CISA
Paul Wiggins, CISSP

DISTRIBUTION LIST

Dr. R. Bowen Loftin, President
Dr. Karan Watson, Provost and Executive Vice President for Academics
Ms. B.J. Crain, Vice President for Finance and Chief Financial Officer
Dr. Rodney McClendon, Vice President for Administration
Mr. Andy Bland, Executive Director - Division of Finance IT Services
Mr. Charley B. Clark, Associate Vice President for University Risk and Compliance