COMMITTEE MEETING MINUTES
of the
Audit, Compliance, and Management Review Committee

OF THE BOARD OF REGENTS

OF

THE UNIVERSITY OF TEXAS SYSTEM

September 28, 2004

Austin, Texas

These Minutes of Committee meetings are taken as a convenience for research purposes and may be verified by tape recordings kept in the Office of the Board of Regents or webcasts available at http://www.utsystem.edu/bor/meetings/minuteslistinghomepage.htm

/s/ Francie A. Frederick
Counsel and Secretary to the Board
January 11, 2005

MINUTES
U. T. Board of Regents
Audit, Compliance, and Management Review Committee
September 28, 2004

The members of the Audit, Compliance, and Management Review Committee of the Board of Regents of The University of Texas System convened at 3:30 p.m. on Tuesday, September 28, 2004, on the 9th Floor of Ashbel Smith Hall, The University of Texas System, 201 West Seventh Street, Austin, Texas, with the following members of the committee in attendance:

Attendance
Regent Estrada, presiding
Vice-Chairman Clements
Vice-Chairman Hunt
Vice-Chairman Krier
Regent Craven

Also present were Regent Barnhill and Counsel and Secretary Frederick.

In accordance with a notice being duly posted with the Secretary of State and there being a quorum present, Chairman Estrada called the meeting to order.

1. U. T. System: Report on the State Auditor's Office financial statement audit for fiscal year ending August 31, 2004

Committee Meeting Information
Presenter(s): *Mr. Chaffin, Mr. Kelton Green, and Mr. Ron Franke*
Status: *Reported*

Agenda Item:

REPORT

Mr. Kelton Green and Mr. Ron Franke, representatives from the State Auditor's Office, reported on their plan to perform financial audit procedures at several U. T. System institutions to express an opinion on the colleges and universities' financial information included in the State of Texas Comprehensive Annual Financial Report as of August 31, 2004. U. T. System represents approximately 60% of this total.

This information is being provided to assist the Audit, Compliance, and Management Review Committee in its oversight responsibility for the U. T. System financial statements.

Discussion at meeting:

Mr. Chaffin reminded the Committee of the upcoming financial audit for Fiscal Year 2005 but said this report concerns Fiscal Year 2004 whereby the State Auditor would be auditing the State of Texas, including a focus on several U. T. System institutions. He introduced Mr. Ron Franke, Audit Manager, Mr. Kelton Green, Managing Senior Auditor, and Ms. Natasha Kelley, all from the State Auditor's Office (SAO).

Mr. Franke said Ms. Carol Smith, another audit manager, was not able to attend this meeting but that he and Ms. Smith would be sharing the responsibility for the overall audit management of the higher education entities portion of the financial work for this year's statewide audit.

Mr. Green reported the audit had begun and there are two main objectives for the Fiscal Year 2004 audit. The first is to issue an opinion on the State of Texas financials for Fiscal Year 2004. The second is to issue an opinion on the college and university portion of those financial statements. He said the auditors will work at U. T. System Administration and at four institutions: U. T. Arlington, U. T. Austin, U. T. Southwestern Medical Center - Dallas, and U. T. Medical Branch - Galveston. He indicated communication will be maintained with individuals at U. T. M. D. Anderson Cancer Center, where Deloitte is conducting an external audit to ensure they are not proposing adjustments to the financial statements that would be significant at the U. T. System level. He reported the SAO has assigned 15 auditors to complete the work at U. T. institutions this year. In total, this group has more than 110 years of audit experience and they will spend an estimated 4,300 hours conducting the work.

Mr. Green indicated the SAO has other teams of auditors conducting work at state agencies and at five other universities around the state that are in the plan this year. They coordinate with other auditors as opportunities arise, in part to avoid duplication in audit coverage. He said work papers that KPMG produced last year were reviewed and he mentioned staying abreast of the Ernst & Young audits of the major UTIMCO investment funds.

Mr. Green explained the risk-based application system known as the Audit Combination and Evaluation System (ACES) to determine line items to audit and thus, where to focus audit efforts. He noted efficiencies will be gained by updating the same line items used last year rather than recreating, and he provided information on those line items.

Mr. Green reported that fieldwork had started at U. T. Arlington and U. T. Southwestern Medical Center – Dallas and fieldwork would begin next week at U. T. Austin. In late October or early November, work would begin at U. T. Medical Branch – Galveston and at U. T. System Administration and all the fieldwork throughout the U. T. System would be completed in January 2005. He said

deliverables for the project are 1) the opinion on the state's financials mentioned earlier, which is due February 28, 2005, and 2) a statewide management letter, planned to be produced in early spring. That letter will include the most significant internal control and dollar issues found in conducting the statewide financial audit. He emphasized issues found during fieldwork would be fully discussed with executive management and findings would be in writing for more significant issues, with a request for a written response.

Mr. Chaffin invited the State Auditor representatives to come back either at the February or May Audit Committee meeting to discuss the findings and the management letter.

2. U. T. System: Report on State Auditor's recommendations regarding protection of research data

Committee Meeting Information
Presenter(s): *Mr. Chaffin, Mr. Dan Updegrove, Mr. Kirk Kirksey, and Mr. Jerry York*
Status: *Reported*

Agenda Item:

REPORT

The State Auditor's Office recently concluded an audit of the protection of research data at three U. T. System institutions: U. T. Austin, U. T. Southwestern Medical Center - Dallas, and U. T. Health Science Center - San Antonio. The audit report was issued in June 2004 and includes several recommendations regarding the need for comprehensive information security programs for research data and improved network security. The report further states that, while issues were noted that increase the risk of loss of research data, no specific instances of research data loss or misuse were identified.

Mr. Dan Updegrove, Vice President for Information Technology at U. T. Austin, Mr. Kirk Kirksey, Vice President for Information Resources at U. T. Southwestern Medical Center - Dallas, and Mr. Jerry York, Vice President and Chief Information Officer at U. T. Health Science Center - San Antonio reported on each institution's response to the State Auditor's report and on actions being taken to resolve the issues noted.

Discussion at meeting:

Mr. Chaffin reported the State Auditor's Office (SAO) performs risk-based audits at the institutions from time to time and in 2003, three information technology (IT) audits were conducted and recommendations issued, while in 2004, similar work was performed at U. T. Health Science Center – San Antonio, U. T. Austin, and U. T.

Southwestern Medical Center – Dallas. He introduced Mr. York, Mr. Updegrove, and Mr. Kirksey to describe the IT challenges at the respective institutions and implementation of recommendations.

Mr. York said he was pleased to present progress on the recent SAO audit, especially since SAO representatives were in attendance. In summarizing protection of information assets, Mr. York referenced the report in the Agenda Book and said the SAO report allowed the institution to reinforce some initiatives that were well underway before the audit and helped to continue to prioritize activities. Over the last three years, the U. T. Health Science Center – San Antonio spent over $1.4 million on information security and has four certified professionals working to protect information. Should they experience a hacking event or a major virus attack, 25 staff members are pulled together to try to resolve the issues.

Mr. York reported that while U. T. Health Science Center – San Antonio is one of the smaller campuses within the U. T. System, 120,000 viruses are blocked every month. Concerning the SAO audit, he said out of the 35 responses provided to the SAO, 12 required technology solutions, unfortunately a few of them were fairly expensive, and 15 require continual reinforcements of policies or procedures that are in place or are being put in place. He said six more tasks have been completed since the report was mailed. Mr. York said responses to the SAO Audit are expected to be fully complete by next spring.

Mr. York said the institution is taking a unique and bold approach to information security by charging departments should their faculty or staff either carelessly or deliberately go against some of the information security policies. He said the approach reinforces the seriousness of the issue and they hope the approach is effective in better protecting information assets.

He said he believes the institution is on track to satisfy the SAO report and noted the real challenge is to stay ahead of the hackers. Since hackers are talented and deliberate, the institution will continue to emphasize information security as a high priority through training and awareness programs. He said they will continue to identify funding to help underwrite some of the sophisticated and expensive technology tools that will provide better protection.

Mr. Kirksey said there are similar challenges at U. T. Southwestern Medical Center – Dallas, with 10,000 users spread over four independent institutions. They electronically store three million patient records, including critical lab results, X-rays, and diagnostic information. Mr. Kirksey explained the institution has begun to give the public access to their medical records via the web.

He described the use of computers in each research laboratory and said IT security is taken seriously. He described the IT program that began in 2000, with the creation of an information security officer who reports to his office. Critical systems have been centralized and he described their disaster recovery program as stellar.

The institution has subscribed for the past three years to a hot site in Chicago. Once a year, programmers travel to Chicago with backup tapes, systems are restored, and operations in critical areas such as clinical and administrative are simulated.

Procedures have been implemented to scan for viruses and he said on a typical weekend, the firewalls stop 90,000 hacker events. Approximately 1,300 viruses are stopped every day with email filters and secure encrypted access has been implemented for wireless access in remote areas. He reported that firewalls are upgraded and the institution has implemented self-auditing.

He commended the State Auditor's Report as a professional work that has been invaluable, because it provides a third eye; a fresh look. He said their main effort in 2004 - 2005, is to technically re-architect the network to provide a series of inner perimeters that become more difficult to break into. In terms of the Audit, he reported there were 34 Audit findings; 7 are complete, 5 are in the final stage and will be completed within the next 30 days, and the rest are underway. He stated they do not necessarily agree with two of the audit findings in particular, but will work with the SAO to reach a compromise.

Mr. Updegrove also expressed appreciation for the opportunity to meet with the Audit Committee. He said U. T. Austin is a research-intensive institution as noted in the SAO report, with some 3,500 research projects ongoing at any one time, many of which make extensive use of computers and network technology. Some of the projects rely exclusively on access to advanced technology and, like the other institutions, they subscribe to the notion of defense in-depth; there is not just a single defense mechanism. For instance, one cannot protect just the PCs and neglect the network, nor can only the interface between the U. T. network and the rest of the Internet be protected with the assumption that everything else is fine. He said the majority of their efforts over last couple of years has been focused on trying to create a safe environment for researchers to carry out their work.

Mr. Updegrove reported the creation in 2001 of the first-ever central information security office that reports directly to him. Sophisticated vulnerability scanning software was licensed to allow assessment of the 40,000 computers on the network for the latest vulnerability. An initiative to replace social security numbers as the university's identification number was launched, but ironically, an unfortunate break-in happened before the project was completed. In 2002, antivirus software and personal firewall software was licensed for campus-wide use including personal computers owned by faculty, students, and staff. In 2003, a program to promote Software Patch Management was launched but, he explained, there is typically a worldwide race between the people who create the patches and the people who create the exploits and there were concerns, such as a given patch insufficiently tested might introduce more problems than it was intended to solve. However, since August 2003, the sophistication and organization of the attacker community around the Internet is so pervasive and so forceful that it is critically important to get patches installed as quickly as possible, even if occasionally they disrupt "business as usual".

Mr. Updegrove said parts of the network have been re-architected to create so-called "quarantine zones" so if a computer is detected as misbehaving, access to the rest of the network and the rest of the Internet would be blocked. He said last year, anti-spam software was licensed and he remarked that was the most popular intervention implemented in the history of IT at U. T. He reported that findings indicate over 80% of the incoming mail for U. T. is fraudulent or spam in nature and anti-spam software has increased productivity. Sophisticated intrusion detection software has also been installed to instantaneously detect the campus computer that is doing something unusual. Mr. Updegrove said increasingly, there is evidence that this is organized criminal activity that can launch attacks on credit card and personal information and beyond. He noted the increasingly hostile environment and they work to secure personal computers at home as well as the campus networks.

In response to a question from Vice-Chairman Krier about how state agencies and campuses interact when a problem is identified, Mr. Updegrove explained the information security officers in the U. T. System meet quarterly and email lists and phone trees are in place and used as a first line of defense both in the state and nationwide. Mr. York clarified the security group has been meeting for 3½ years and there were 50 people at the most recent meeting wherein best practices were shared. Vice-Chairman Krier noted this as another great example of collaboration.

Regent Estrada asked if there were observations from the State Auditor's Office on this process and Mr. Ron Franke said he is encouraged by management of the difficult IT challenges at the three institutions and he commented on the constant balance that is required to be maintained between the desire to have an absolutely secure environment and the need to have an open academic, medical, and research environment. He applauded representatives from the three institutions for taking IT security seriously, making it a priority, and doing their best to tackle it. He said, "Security is not a destination, it is a journey. And everyday it starts over again."

Committee Chairman Estrada expressed appreciation to the presenters, saying their partnership in trying to address these issues has been helpful.

3. U. T. System: Approval of U. T. System Internal Audit Plan for Fiscal Year 2005

Committee Meeting Information

Presenter(s): *Mr. Chaffin*
Status: *Approved*

Agenda Item:

RECOMMENDATION

It was recommended that the Audit, Compliance, and Management Review Committee approve the proposed U. T. System-wide Internal Audit Plan for Fiscal Year 2005 and recommend the Plan to the U. T. System Board of Regents for approval at the November 2004 meeting. Development of the Internal Audit Plan is based on risk assessments performed at each institution. Implementation of the Plan will be coordinated with the institutional auditors.

BACKGROUND INFORMATION

Institutional Audit Plans, compiled by the internal audit departments after input and guidance from the System Audit Office and the institution's management and Internal Audit Committee, were submitted to all Internal Audit Committees and institutional presidents for review and comments.

The Chief Audit Executive provided feedback by conducting audit hearings with each institution. After the review process, each Internal Audit Committee formally approved its institution's Plan.

Discussion at Meeting:

Mr. Chaffin reminded members of the Committee there are internal auditors and internal audit committees at each U. T. System institution, and independent members are being arranged to be a part of internal audit committees at many of the institutions. The audit planning process begins in the spring with development of a risk assessment. Through that entire process, the internal audit departments prepare audit plans that are reviewed at U. T. System Administration in an audit hearing. In conjunction with management, the proposed audit plan is brought forward by the audit committee. Mr. Chaffin said the audit plan is divided in two parts; the full plan and the priority plan, which is 80% of the full plan and is a commitment on the part of the institution to execute that 80%, no matter what. Mr. Chaffin explained the goal is to complete 100% of the plan.

He said the plan before the Committee is the priority plan. He explained the details of the plan as found on Page 7 of the Agenda Book, including the 127,000 hours divided into key financial and operating information, a significant portion of which is allocated to the first ever financial audit of the U. T. System. That audit has been divided into two parts that will entail approximately 15,000 hours of internal audit work:

- *at the large institutions, audit directors will be working directly under the guidance of Deloitte; and*

- *at the smaller institutions, audit directors will be executing on their own the audit programs provided by Deloitte.*

Mr. Chaffin mentioned that compliance remains a significant part of the work and the rules continue to get more complex. He said this year the Governor came forward with a fraud initiative that is being responded to this week, with emphasis on certain areas such as contract and information technology compliance. He said another area is core business processes regarding implementation of enterprise-wide risk management. He said the intent is to audit key areas within operations, particularly the most risky. He said internal controls in a department may be audited when there is a change in management to ensure internal controls are strong.

Mr. Chaffin said he would monitor the progress of completion of the audit plans on a quarterly basis and report back to the Committee, providing feedback.

Committee Chairman Estrada asked if U. T. Health Science Center - Houston would have an outside audit? Mr. Chaffin said the institution's internal audit director resigned in late June effective early July and a new internal audit director from U. T. M. D. Anderson Cancer Center was hired and is building her staff. He intends to present the audit plan for U. T. Health Science Center – Houston at the next Committee meeting.

Regent Estrada asked if hours reflected in the Agenda Item for U. T. M. D. Anderson Cancer Center were over and above the outside audit and Mr. Chaffin responded yes, these are internal audit hours.

Mr. Chaffin said that as part of The University of Texas Investment Management Company (UTIMCO) Working Group, there was a recommendation that more internal audit work be devoted to UTIMCO. He noted the plan includes approximately 2,000 hours of audit work and an outstanding individual with background in investments has been hired. He said an audit of several areas including fees had begun and he believes all the risks are covered by the internal audit work, the State Auditor's work, and the Deloitte financial audit.

RECESS TO EXECUTIVE SESSION.--At 4:10 p.m., Committee Chairman Estrada announced the Audit, Compliance, and Management Review Committee would recess to convene in Executive Session pursuant to Texas Government Code Sections 551.071 and 551.074 to consider matters listed on the Executive Session agenda as follows:

1. U. T. Board of Regents: Personnel Matters Relating to Appointment, Employment, Evaluation, Assignment, Duties, Discipline, or Dismissal of Officers or Employees – Texas Government Code Section 551.074

   U. T. System: Evaluation and duties of System and institutional employees involved in audit and compliance functions

2. U. T. Board of Regents: Consultation with Attorney Regarding Legal Matters or Pending and/or Contemplated Litigation or Settlement Offers – Texas Government Code Section 551.071

RECONVENE.--At 4:20 p.m., the Board reconvened in open session. No action was taken on any item listed on the Executive Session agenda.

ADJOURNMENT

Committee Chairman Estrada announced that the purpose for which this meeting was called had been completed, and the meeting was duly adjourned at 4:20 p.m.