The University of Texas at Dallas
Institutional Compliance Program
Quarterly Report
For the Quarter Ended November 30, 2006

Section I – Organizational Matters

- The quarterly meeting of the Compliance Subcommittee was held on November 29, 2006.
- The quarterly meeting of the Audit and Compliance Committee was held on December 8, 2006.
- The Compliance Officer, Marianne Rutledge, resigned effective November 3, 2006. A search for a new Compliance Officer is underway. The Search Committee is currently discussing employment opportunities with one of the candidates and hopes to have a final decision before the holiday break.
- Executive Compliance Committee training was conducted during the Audit and Compliance Committee meeting held during the fourth quarter of 2005. The Subcommittee also received a copy of the training session during their November 2006 meeting.

Section II - Risk Assessment, Monitoring Activities and Specialized Training (Performed by Responsible Party)

Reminder: This section should contain information on the identified significant institutional risks and monitoring activities performed to mitigate those risks, ***conducted primarily by the responsible party****. For your* ***six most critical*** *"A" compliance risks areas, include the responsible party, key "A" risks identified, risk monitoring activities performed by the responsible party/designate, and specialized training conducted. You may also add other risk areas that you consider to be critical to your institution.*

Additionally*, each quarter the* ***System-wide Compliance Office will identify one specific "A" risk area or specific risk*** *for you to provide the requested information on. In total,* ***please include no more than 10 "A" risk areas***

The "A" risk areas should be ranked and communicated in order of their significance from highest to lowest. The following format is recommended:

High-Risk Area #1: Information Security
Responsible Party: Information Security Administrator
Key "A" risk(s) identified:

- TAC 202.70[1]. Texas Administrative Code, Information Security Standards for Institutions of Higher Education. All institutions of higher education are required to have an information resources security program consistent with TAC 202 standards, and the President is responsible for the protection of information resources. Institutions of higher education must ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.
- Scanning (Imaging System). Unauthorized access of confidential and sensitive data on scanning systems University-wide. The methods used to access these systems are not secure.
- Server Security. Requirements for installing and maintaining the integrity of servers to avoid system/data corruption on the network.

Key Monitoring Activities:

- TAC 202: We monitor incidents and resolve at they occur.
- Server Security: We monitor for compromised servers and block them from the network until they can be cleaned. We do some proactive scanning and are planning more.
- Scanning: We monitor for compromised servers and block them from the network until they can be cleaned. We do some proactive scanning and are planning more.

Specialized Training:

- Scanning & Server Security: None.
- TAC 202: Carl Ratliff attended the UTINFOSEC meeting (group of all security officers of UT System institutions), hosted in Galveston in September.

High-Risk Area #2: FERPA
Responsible Party: Assistant VP for Student Affairs
Key "A" risk(s) identified:

- Inappropriate release of student confidential information resulting in loss of ability to handle:
  - Student financial aid
  - Identity theft
  - Negative public regulations

Key Monitoring Activities:

- The Registrar continued to monitor for compliance through periodic walk-arounds and observations in various offices on campus.

- The first meeting of the FERPA Compliance Subcommittee was held on November 2, 2006. Committee members reviewed FERPA regulations, forms and processes and discussed ways we can provide for more

[1] http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=202&sch=C&rl=Y

education and more comprehensive monitoring of FERPA compliance across campus.

Specialized Training:

- Registrar's staff received refresher training on FERPA.

High-Risk Area #3: HIPAA Security Rule (Callier Center)
Responsible Party: Information Security Administrator
Key "A" risk(s) identified:

- Lack of security resulting in unauthorized access to personal health information (PHI), potential fines and criminal charges.

Key Monitoring Activities:

- As described in the HIPAA security policies.

Specialized Training:

- None.

High-Risk Area #4: Social Security Number (SSN) Protection
Responsible Party: Assistant VP for Human Resources Management
Key "A" risk(s) identified:

- Identity theft
- Violation of System regulations
- Violation of federal laws

Key Monitoring Activities:

- HR staff reviewed Training Post logs and follows up with any employees who have not completed their training in a timely manner.

Specialized Training:

- None.

High-Risk Area #5: Environmental Health and Safety (EH & S)
Responsible Party: Director of EH & S
Key "A" risk(s) identified:

- Occupational & General Safety
- Environmental Management
- Fire and Life Safety
- Laboratory Safety
- Industrial Hygiene

Key Monitoring Activities:

Specialized Training:

- EH&S Staff attended the 8- hour Hazwoper Refresher Class.
- The EHS Director averages about two staff meetings per month to train staff our requirements and action plans.

High-Risk Area #6: Student Financial Aid
Responsible Party: Director of Student Financial Aid
Key "A" risk(s) identified:

- Unofficial withdrawals – return funds "not earned" by the student to appropriate program source.
- Overawarding – return of federal funds due to overawarding.

Key Monitoring Activities:

- Random selection of five records on Ready to Award list dated 10/11/06 was done. All components of file reviewed, records reviewed and processed correctly with no non-compliance issues noted.

Specialized Training:

- October 11-13 State Financial Aid Conference attended by Cathy Coursey, Mary Roffino, Paula Baxter, James Hubener, James Dorman, Donna Everson.
- November 20, 2006 DOE HERA Updates Workshop attended by Cathy Coursey, Rich Cummings, Mary Roffino, Beverly Wilson, Angela Craig, James Hubener, Paula Baxter, Sarah Hernandez, Donna Everson

High-Risk Area of Concern to UTD: Research Compliance. Time and Effort Reporting
Responsible Party: Associate VP for Business Affairs & Controller
Key "A" risks(s) identified:

- Lack of effort reporting and/or non-compliance with OMB Circular A-21 resulting in repayment of federal funds.

Key Monitoring Activities:

- None. However, the new time and effort certification reporting system is being tested. Rollout is expected within the next quarter.

Specialized Training:

- Doug Shedd and Merrie Tabbert attended the NCURA Conference in November and September, respectively, and both had sessions on Time and Effort Reporting.
- Mary Carter attended a policy development workshop in Austin in November 2006 that included a discussion of Time and Effort Reporting.

Section III – Monitoring and Assurance Activities (Performed by Compliance Office)

Reminder: Please report summary information pertaining to monitoring and assurance activities (such as certifications, inspections, peer reviews, and audits) ***performed by the compliance office/designate during the quarter*** *on any of your institution's high risk compliance "A" risks to validate the robustness and effectiveness of established controls.*

Include monitoring and assurance activities performed, any significant findings identified, and provide the compliance office's assessment of the control structure as either "well controlled", "opportunity for enhancement", or "significant opportunity for enhancement."

High-Risk Area #1: Information Security
Assessment of Control Structure: Opportunity for enhancement
Assurance Activities Conducted:

- Inspection of Server Management 10/5/06. Performed usual inspection procedures. See below.
- Internal Audit: In process of a TAC 202 audit, to be completed by December 2006.

Significant Findings:

- The Risk Assessment and Monitoring Plan (RAMP) for Server Management needs to be updated to address additional areas of concern and the activities performed by Information Security to ensure compliance with server management and registration policies.

High-Risk Area #2: FERPA
Assessment of Control Structure: Opportunity for enhancement
Assurance Activities Conducted:

- Inspection 10/4/06.

Significant Findings:

- RAMP needs to be revised.

High-Risk Area #3: HIPAA Security Rule (Callier Center)
Assessment of Control Structure: Opportunity for enhancement
Assurance Activities Conducted:

- None during 1st Quarter FY 2007.

Significant Findings:

- No significant findings – minor revisions to RAMP suggested in 4th Quarter 2006 inspection.

High-Risk Area #4: SSN Protection
Assessment of Control Structure: Opportunity for enhancement
Assurance Activities Conducted:

- None during the 1st Quarter of FY 2007.

Significant Findings:

- Per Internal Audit performed in FY 2006, RAMP needs to be updated and monitoring needs to be performed in all areas of the campus (not just HR). Current monitoring is not sufficient. Per discussions with HR, recommendation is still in process.

High-Risk Area #5: EH & S
Assessment of Control Structure: Opportunity for enhancement
Assurance Activities Conducted:

- Monthly meetings with Director of EH & S, Compliance Officer, and Compliance Coordinator to discuss Risk Assessment and Monitoring Plans (RAMPS).
- Working with EH & S Director on monitoring for revised RAMPS and how to complete the quarterly reports.
- None for 1st quarter FY 2007.

Significant Findings:

- RAMPS need to be revised and monitoring needs to take place for labs per previous Internal Audit report, and recommendation considered significant to UTD operations. Being monitored quarterly by Internal Audit and Audit, Compliance, and Management Review Committee (ACMR) of the U. T. System Board of Regents. RAMPS have been revised, and Internal Audit planned for 3rd quarter FY 2007.
- Quarterly reports show no evidence of monitoring due to new staff and organizational changes.

High-Risk Area #6: Financial Aid
Assessment of Control Structure: Well controlled.
Assurance Activities Conducted:

- State Auditor's Office audit in process during first quarter of FY 2007.

Significant Findings:

- None to date.

High-Risk Area of Concern to UTD: Research Compliance. Time and Effort Reporting
Assessment of Control Structure: Opportunity for enhancement.
Assurance Activities Conducted:

- Audit and Compliance meetings with Responsible Person regarding progress on training and implementation on new Business Procedure Memorandum No. 76.

Section IV – General Compliance Training Activities

- 91% of the employees scheduled to take general and/or new employee training during calendar year completed their assigned training as of November 2006.
- The Compliance Officer presented a brief Introduction to Compliance during New Employee Orientation meetings until the end of October 2006. Currently, the Office of Human Resources Management is conducting the Introduction to Compliance portion of the training that is held every two weeks.

Section V – Action Plan Activities

The following Action Plan items were implemented during the quarter just ended:

- Conducted one-on-one meeting with responsible parties for EH & S and Research Compliance.
- Conducted quarterly meetings with the Compliance Subcommittee.

- Conducted quarterly meetings with the Executive Audit and Compliance Committee and discussed reports on the status of high-risk areas and new issues.
- Completed a Level of Effort analysis and met with Information Resources on the Breeze project to replace the existing compliance training program, The Training Post.
- Selected and received the Audit and Compliance Committee's approval for the General Compliance Training modules to be required for all benefit-eligible employees for FY 2007.
- Monitored and reported on completion of required compliance training.
- Prepared the FY 2007 Compliance Action Plan for UT System.
- Provided monthly reports to UT System.
- Reported on the status and proposed changes to high-risk areas and compliance issues to the Audit and Compliance Committee.
- Began enhancement of High-Risk List by adding columns for assurance activities and assessment of risk.

Significant Action Plan scope changes during the quarter included:

- Due to the resignation of the Compliance Officer, the updates of the Management Responsibilities Handbook, Compliance Manual, and quarterly Audit and Compliance Newsletter were postponed until a new Compliance Officer could be hired.
- Due to other Information Resources priorities, and due to difficulties obtaining support from the vendor, the Breeze project was delayed. The Breeze project team decided to look into WebCT as an alternative reporting tool, and a meeting has been scheduled in December 2006 to discuss the project with the employees responsible for WebCT at UTD. Resources in Information Resources have been identified to begin approximately 60% time in January 2007, pending other priorities.

The following procedures are used in all inspections performed by the Compliance Office.

COMPLIANCE INSPECTION PLAN	Done	Comments
A. *Gain an Understanding of the Compliance Program*		
1. Review previous inspection report(s)/ audit reports.		
2. Review the RAMP for the High Risk Area.		
3. Review any applicable laws or regulations for the high risk area.		
a. Check for any revisions to the applicable law/regulations.		
b. Check for any new legislation that would have an effect on the high-risk.		
4. Review RAMP with Responsible Person.		
5. If necessary, request updated RAMP from Responsible Person.		
B. *Test the Compliance Program*		
1. Method of Monitoring		
a. Determine if the responsible person is effectively monitoring compliance with the program as stated in the monitoring plan.		
b. Review documentation indicated in method of monitoring to ensure it exists and is being used as described.		
c. Judgmentally select samples for each of the monitoring controls and perform testing to ensure compliance with the monitoring plan.		
2. Training		
a. Determine if training is being performed in accordance with the training plan.		
b. Review documentation to ensure that training is being performed.		
c. Judgmentally select samples for each of the monitoring controls and perform testing to ensure compliance with the monitoring plan.		
3. Reporting		

a. Determine if reporting is being performed in accordance with the reporting plan.		
b. Review documentation to ensure that reporting is being performed.		
C. Final Procedures		
1. Perform additional procedures as necessary.		
2. Document results in a Memo to the Responsible Person.		