TABLE OF CONTENTS
FOR
AUDIT, COMPLIANCE, AND MANAGEMENT
REVIEW COMMITTEE

Brenda Pejovich, Chairman
Wallace L. Hall, Jr.
R. Steven Hicks
Jeffery D. Hildebrand
Robert L. Stillwell

Committee Meeting: 11/14/2013
Board Meeting: 11/14/2013
Austin, Texas

A. CONVENE
(Conference Room, Ashbel Smith Hall, 9th Floor) 8:30 a.m. Chairman Pejovich

B. RECESS TO EXECUTIVE SESSION PURSUANT TO TEXAS GOVERNMENT CODE, CHAPTER 551

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: Discussion with the Chief Audit Executive concerning personnel matters relating to appointment, employment, evaluation, assignment, duties, discipline, or dismissal of individual System Administration and institutional officers or employees involved in internal audit functions Mr. Peppers

C. RECONVENE IN OPEN SESSION
(Board Room, Ashbel Smith Hall, 9th Floor) 8:45 a.m.

1. U. T. System Board of Regents: Discussion and appropriate action regarding Consent Agenda items, if any, referred for Committee consideration 8:45 a.m. Action Action 17

2. U. T. System: Update on the implementation of initiatives to address recommendations from the Report on the Strategic Assessment of the U. T. System Internal Audit Services performed by Deloitte 8:47 a.m. Report/Discussion Not on Agenda 18

3. U. T. System: Report on the Systemwide internal audit activities, including results of the executive travel and entertainment, laptop encryption and IT inventory, and practice plan audits, and update on the Systemwide internal audit of development activities 8:50 a.m. Report/Discussion Not on Agenda 19


D. ADJOURN 9:15 a.m.
1. **U. T. System Board of Regents: Discussion and appropriate action regarding Consent Agenda items, if any, referred for Committee consideration**

**RECOMMENDATION**

The proposed Consent Agenda is located at the back of the book.
2. **U. T. System: Update on implementation of initiatives to address recommendations from the Report on the Strategic Assessment of the U. T. System Internal Audit Services performed by Deloitte**

**REPORT**

Chief Audit Executive Peppers will provide an update on implementation of initiatives developed to address the recommendations from the report on the Strategic Assessment of the U. T. System Internal Audit Services performed by Deloitte, which was presented at the May 8, 2013 Audit, Compliance, and Management Review Committee meeting. The 17 recommendations have been organized into eight key initiatives to be implemented over a three-year period as follows:

**Governance**

- Strengthen institutional audit committee independence and capability
- Assess Systemwide and institutional risk management
- Provide resources for governance

**Processes, Resources, and Capability Development**

- Organize mission and values into objectives, models, and priorities
- Enhance risk assessment methodology
- Develop audit and reporting models
- Quantify and improve team competency

**Success and Sustained Quality**

- Align internal audit metrics and quality program with improvement plans
3. **U. T. System: Report on the Systemwide internal audit activities, including results of the executive travel and entertainment, laptop encryption and IT inventory, and practice plan audits, and update on the Systemwide internal audit of development activities**

**REPORT**

Chief Audit Executive Peppers will report on the Executive Travel and Entertainment Expenses audits and the Laptop Encryption and IT Inventory audits that were conducted at U. T. System Administration and each of the U. T. System institutions. He will also report on the practice plan audits that were performed at the U. T. System health institutions. Summaries of the results for these audits were provided to the Regents prior to the meeting.

Chief Audit Executive Peppers will provide an update on the Systemwide internal audit of development activities performed by the U. T. System Audit Office. Reports for U. T. System, U. T. System Administration, and U. T. M. D. Anderson Cancer Center have been issued and were provided to the Regents prior to the meeting. He will also present the results of the U. T. Austin Law School Foundation Special Request Project conducted by the System Audit Office, for which the report was issued and previously provided to the Regents.

**REPORT**


**BACKGROUND INFORMATION**

Following a November 10, 2011 report to the Board by Deloitte on its comprehensive information security compliance effectiveness review of the U. T. System, the Board approved the allocation of $34,872,000 of Available University Funds to invest in information security compliance enhancements across the U. T. System and to secure the U. T. Research Cyberinfrastructure.

The Office of Systemwide Compliance administers the investment of these funds through a centrally managed program and is to submit annual reports on progress to the Chancellor and to the Board. This is the second Annual Report.
ANNUAL REPORT ON INFORMATION SECURITY
COMPLIANCE ENHANCEMENTS

Audit, Compliance, and Management Review Committee
U. T. System Board of Regents’ Meeting

November 2013

Mr. Lewis Watkins, U. T. System Chief Information Security Officer
U.T. System
Common Risks

Risk 1 - Mobile Device Security
Risk 2 - Decentralized IT
Risk 3 - Network Security
Risk 4 - Logging and Monitoring
Risk 5 - Disaster Recovery
Risk 6 - Inconsistent Risk Assessment
Risk 7 - Unencrypted Backup Tapes
Risk 8 - Third-party Risk Management
Risk 9 - Software Development & Configuration Mgt.
Risk 10 - Physical Security
Risk 11 - Identity and Access Management
Risk 12 - Training and Awareness
Risk 13 - CISO Authority and Culture

Information Security gaps posing highest risk across the U. T. System
High Risk Area 1: Mobile Device Security

• Completed laptop encryption Systemwide

• Purchased mobile device management software for Systemwide use to enforce iPad, iPhone, and Android encryption and configuration management

• Deployed encrypted thumb drives to U. T. System faculty and staff using/maintaining confidential information

• Launched a Systemwide Network Access Control Working Group led by U. T. San Antonio
High Risk Area 2: Decentralized IT

• Completed two technology consolidation projects:
  – U. T. Austin centralized 1000+ servers
  – U. T. Health Science Center - San Antonio centralized 177 servers

• Completed centralization of access management at U. T. Southwestern Medical Center
High Risk Area 3: Network Security

- Completed U. T. San Antonio network upgrade
- Started segmentation of critical servers at U. T. Health Science Center - Tyler
- Completed enterprise firewall upgrade at U. T. Pan American
- Completed U. T. Health Science Center - San Antonio wireless network upgrade
High Risk Area 4: Logging and Monitoring

- Purchased patient privacy monitoring software for U. T. health institutions’ use
- Launched a Security Incident and Event Monitoring Working Group led by U. T. Health Science Center - Houston
High Risk Area 5: Disaster Recovery

• Disaster Recovery for the Arlington Regional Data Center (ARDC)
  — Backup processing for Shared PeopleSoft applications
  — U. T. Arlington failover capabilities

• Disaster Recovery Plan and co-location at a remote location for UTShare and Texas Student Information System
  — Systems are used by multiple institutions
High Risk Area 6: Inconsistent Risk Assessment

- **Risk Assessment Consistency:**
  - Established a U. T. System Risk Assessment Framework based on the National Institute of Standards and Technology
  - Purchased risk assessment software for Systemwide use
  - Started pilot deployment in five early adopter institutions

- **Third-Party Risk Assessment:**
  - Established a third-party risk assessment process based on U. T. System Risk Management Framework
  - Important for outsourcing and collaborations arrangements
## Project Funding by Risk Area

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Projects Addressing High Risks Affecting Many Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security</td>
<td>$5,036,552</td>
</tr>
<tr>
<td>Risk Management</td>
<td>$3,453,996</td>
</tr>
<tr>
<td>Monitoring and Logging</td>
<td>$3,449,807</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>$3,301,497</td>
</tr>
<tr>
<td>Decentralized IT Migration</td>
<td>$2,681,555</td>
</tr>
<tr>
<td>Patient Privacy Monitoring</td>
<td>$2,306,992</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>$1,465,029</td>
</tr>
<tr>
<td>Mobile Device Security</td>
<td>$1,017,857</td>
</tr>
<tr>
<td>Encryption</td>
<td>$1,016,830</td>
</tr>
<tr>
<td>Infrastructure Upgrade</td>
<td>$868,183</td>
</tr>
<tr>
<td>Physical Security</td>
<td>$787,684</td>
</tr>
<tr>
<td>Identity Management</td>
<td>$556,398</td>
</tr>
<tr>
<td>Backup</td>
<td>$345,950</td>
</tr>
<tr>
<td>Training</td>
<td>$250,000</td>
</tr>
<tr>
<td>Business Process Improvement</td>
<td>$98,530</td>
</tr>
<tr>
<td>Application Security</td>
<td>$75,990</td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>$33,541</td>
</tr>
<tr>
<td>Governance</td>
<td>$10,090</td>
</tr>
</tbody>
</table>

*Meeting of the U. T. System Board of Regents - Audit, Compliance, and Management Review Committee*
Funds Allocation to Date

- $17,987,463 (61%)
- $8,769,017 (30%)
- $2,498,520 (9%)
Active and Completed Projects by Activity Area

- Policy Development: 14 Active, 21 Completed
- Business Process Improvement: 19 Active, 16 Completed
- Network Security: 17 Active, 9 Completed
- Risk Management: 20 Active, 5 Completed
- Training: 15 Active, 4 Completed
- Business Process Analysis: 6 Active, 5 Completed
- Physical Security: 9 Active, 4 Completed
- Monitoring and Logging: 12 Active, 3 Completed
- Mobile Device Security: 9 Active, 5 Completed
- Encryption: 4 Active, 10 Completed
- Disaster Recovery: 11 Active, 2 Completed
- Decentralized IT Migration: 6 Active, 2 Completed
- Patient Privacy Monitoring: 5 Active
- Infrastructure Upgrade: 1 Active, 4 Completed
- Identity Management: 5 Active
- Access Control: 3 Active, 1 Completed
- Software Development Life Cycle: 2 Active, 1 Completed
- Data Loss Prevention: 3 Active
- Configuration Management: 1 Active, 2 Completed
- Application Security: 2 Active, 1 Completed
- Vulnerability Scanning: 1 Active, 1 Completed
- Governance: 1 Active
- Backup: 1 Active
Active and Completed Projects by Institution

<table>
<thead>
<tr>
<th>Institution</th>
<th>Active Projects</th>
<th>Completed Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>U. T. Arlington</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>U. T. Austin</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>U. T. Brownsville</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>U. T. Dallas</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>U. T. El Paso</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>U. T. Pan American</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>U. T. Permian Basin</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>U. T. San Antonio</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>U. T. Tyler</td>
<td>14</td>
<td>18</td>
</tr>
<tr>
<td>U. T. Southwestern</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>U. T. Medical Branch</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>U. T. HSC Houston</td>
<td>13</td>
<td>7</td>
</tr>
<tr>
<td>U. T. HSC San Antonio</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>U. T. MDACC</td>
<td>14</td>
<td>24</td>
</tr>
<tr>
<td>U. T. HSC Tyler</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>U. T. System Administration</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Multi-Institutional Projects</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>UTIMCO</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Common Infrastructures</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Project Progress Summary

**Current Project Status**
- Active Projects: 162 (37%)
- Completed Projects: 163 (38%)
- Pending Projects: 110 (25%)

Total Identified Projects: 435

**High Priority Project Completion Status**
- Low and Medium Priority Projects: 294 (68%)
- High-Priority Projects: 141 (32%)

**Projects Underway**
- October 2012: 151
- October 2013: 163

**Cumulative Projects Completed**
- October 2012: 45
- October 2013: 110
Multi-Institution Projects Completed and In Process

- **Mobile Device Management**
  - ✓ Laptop encryption
  - ✓ Encrypted thumb drives
  - ✓ iPhones, iPads, and Androids
    - Network access control

- **Risk Management**
  - IT risk assessments
  - Third-party assessments

- **Training**
  - Technical training
  - User training

- **Logging and Monitoring**
  - Patient privacy
  - Data discovery
    - Security events
Common Infrastructures

• Hired an Information Security Officer for Common Use Information Resources
  – Work with Resource Manager
  – Identify control gaps
  – Define compliance strategies
  – Establish program metrics

• Deployed U. T. Research Cyber Infrastructure Perimeter Security Devices

• Completed Information Security Assessment for Texas Advanced Computing Center and ARDC
  – Are they electronic protected health information-ready?
U. T. System Security Profile is Maturing

• **Improved Security**
  – Laptop encryption minimizes the number of reportable security breaches
  – Mobile device management provides security standards and secure configurations for mobile devices connecting to institutional networks

• **Alignment**
  – Projects support the Framework for Advancing Excellence
  – U. T. System Risk Management Framework provides a common methodology to assess, report, and aggregate information security risk across all institutions

• **Cultural Shift**
  – Executive management is considering and, in cases, requiring centralization of critical assets
  – Institutions are increasingly considering collaboration and shared strategies to address security

• **Efficiency**
  – Systemwide purchasing and leveraging the U. T. System Supply Alliance generates considerable savings to the U. T. System