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

Committee Meeting: 8/24/2022
Board Meeting: 8/25/2022
Austin, Texas

Nolan Perez, Chairman
Christina Melton Crain
Jodie Lee Jiles
Janiece Longoria
Kelcy L. Warren
Rad Weaver

<table>
<thead>
<tr>
<th>Committee Meeting</th>
<th>Board Meeting</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convene</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:45 p.m.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chairman Perez</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. **U. T. System Board of Regents: Discussion and appropriate action regarding Consent Agenda items, if any, assigned for Committee consideration**

2. **U. T. System: Discussion of Systemwide internal audit activities, including updates on the Systemwide Cancer Prevention and Research Institute of Texas (CPRIT) grants assurance work, the presidential travel, entertainment, and university residence maintenance expenses audit, and the Fiscal Year 2022 Annual Audit Plan status**

3. **U. T. System: Approval of non-audit services to be performed by U. T. System's external audit firm, Deloitte & Touche LLP, for intellectual property license royalty audits to be utilized by any interested U. T. institution**


5. **U. T. System: Discussion and appropriate action regarding request for additional funding of $18,500,000 including $8,500,000 from Available University Funds (AUF) and $10,000,000 from Permanent University Fund (PUF) Bond Proceeds to fund the strategic security services provided to U. T. System by U. T. Austin and to conduct periodic assessments and exercises at the institutions for the period FY24-FY28**

Adjourn

2:15 p.m.
1. **U. T. System Board of Regents: Discussion and appropriate action regarding Consent Agenda items, if any, assigned for Committee consideration**

   **RECOMMENDATION**

   The proposed Consent Agenda items assigned to this Committee are **Items 3 - 4**.
2. **U. T. System: Discussion of Systemwide internal audit activities, including updates on the Systemwide Cancer Prevention and Research Institute of Texas (CPRIT) grants assurance work, the presidential travel, entertainment, and university residence maintenance expenses audit, and the Fiscal Year 2022 Annual Audit Plan status**

Chief Audit Executive Peppers will report on the assurance work conducted by external providers on the Cancer Prevention and Research Institute of Texas (CPRIT) grant activity at U. T. institutions. Additionally, Mr. Peppers will provide an update on the presidential travel, entertainment, and university residence maintenance expenses audit and the Fiscal Year 2022 Annual Audit Plan status as of May 31, 2022. A summary of the CPRIT assurance work, presidential expenses audit results, and details on the plan status were provided to the Audit, Compliance, and Risk Management Committee members prior to the meeting.

**BACKGROUND INFORMATION**

Deloitte & Touche LLP was engaged to conduct audits of FY 2021 CPRIT grant activity for six U. T. institutions. Four other U. T. institutions engaged Weaver & Tidwell to perform agreed upon procedures of FY 2021 CPRIT grant activity.
3. **U. T. System: Approval of non-audit services to be performed by U. T. System's external audit firm, Deloitte & Touche LLP, for intellectual property license royalty audits to be utilized by any interested U. T. institution**

**RECOMMENDATION**

It is recommended that approval be given by the Audit, Compliance, and Risk Management Committee (ACRMC) for U. T. System's external audit firm, Deloitte & Touche LLP, to contract with interested U. T. institutions through a master services agreement for the performance of intellectual property license royalty audits.

**BACKGROUND INFORMATION**

The current external audit firm engaged by the U. T. System Board of Regents to provide audit services is Deloitte & Touche LLP. Audit services are those provided for the purpose of expressing an opinion on the financial statements of U. T. System or any of the institutions.

Regents' Rule 20402, Section 2.1 states, "The U. T. System and the institutions may not engage the external audit firm to perform non-audit services unless the proposed engagement is reviewed and approved by the ACRMC."

Institutions who engage for these services will provide the source funds. Additional information on this project was provided to members of the ACRMC prior to the meeting.

**RECOMMENDATION**

Chief Audit Executive Peppers will present the proposed Fiscal Year 2023 U. T. Systemwide Annual Audit Plan (Audit Plan) using the PowerPoint set forth on the following pages and will recommend its approval. Development of the Audit Plan is based on risk assessments performed at each institution. Implementation of the Audit Plan will be coordinated with the institutional auditors. The Audit Plan executive summary is set forth on the pages following the PowerPoint. Additionally, the detailed annual audit plans were provided to the Audit, Compliance, and Risk Management Committee members prior to the meeting.

**BACKGROUND INFORMATION**

Institutional audit plans, compiled by the internal audit departments after input and guidance from the U. T. System Audit Office, the Offices of Academic or Health Affairs, and the institution's management and institutional internal audit committee, were submitted to the respective institutional internal audit committee and institutional president for review and comments. Also, the U. T. System Chief Audit Executive provided feedback by conducting audit plan presentations with each institution. After the review process, each institutional internal audit committee formally approved its institution's audit plan.
U. T. Systemwide FY 2023 Annual Audit Plan

Mr. J. Michael Peppers, U. T. System Chief Audit Executive

U. T. System Board of Regents Meeting
Audit, Compliance, and Risk Management Committee
August 2022
Overall Audit Plan Process

Systemwide Methodology
- Risk Assessment
- Plan Development
- Format and Content

Review of Audit Plans
- Institutional Management & Stakeholders
- System Audit Office
- Offices of Academic and Health Affairs

Approval of Audit Plans
- Institutional Internal Audit Committees
- Audit, Compliance, and Risk Management Committee
FY 2023 Annual Work Plans

• Internal audit work plans across the System:
  – 46% Assurance Engagements
  – 15% Advisory and Consulting Engagements

• Reserve hours to stay agile and responsive to management needs

• Diverse topics to maximize coverage of risk areas

• Commonality in high-risk area topics
Most Common Topics

- Ensure expenditure compliance with grant or contract-specific requirements, including:
  - Evaluating processes and controls, policy and procedures
Most Common Topics (cont.)

Foreign Influence

- Assess controls to protect research and intellectual property from inappropriate foreign influence:
  - Data security
  - Identity and access management
  - Disclosure requirements
  - Physical equipment/materials
Most Common Topics (cont.)

- Assess processes, controls, and procedures for timely completion of construction projects, accurate billing, and change order management
- Facilities management: Evaluate procedures and risks around deferred maintenance
Most Common Topics (cont.)

- Evaluate processes and controls around various aspects of the medical services revenue cycle, including:
  - Billing practices
  - Charge capture for services provided
  - Collections
Most Common Topics (cont.)

- Verify timely processes and controls around employee onboarding/offboarding:
  - Access management (physical/digital)
  - Compliance with policy requirements
  - Hiring practices (recruitment, background checks, etc.)
  - Onboarding training
  - Offboarding benefits/payouts
Other Common Topics

- Account Reconciliation
- Segregation of Duties
- Enterprise Risk Management
- Purchasing/Supply Chain
- Accounts Payable/Disbursements
- Contracting
- Controlled Substances Management
- Payroll
Common Topics for Required Engagements

- Procurement Compliance
- Annual Financial Report
- NCAA Compliance
- Institutional Facilities Inventory
- Various Grants
Most Common IT Topics

- Disaster recovery & business continuity plans
- Ransomware and backup process
- Decentralized IT disaster Recovery preparedness

Disaster Recovery/ Business Continuity
Most Common IT Topics (cont.)

- Cybersecurity protection and incident response
- Identity and access management
- Cloud/3\textsuperscript{rd} party security \textit{(including TX-RAMP compliance)}
- Data governance and data management \textit{(including Senate Bill 475 compliance)}
Other Common IT Topics

- Decentralized IT
- IT Asset Management
- Electronic Health Records
Systemwide Risk Count vs. Audit Hours by Taxonomy

[Diagram showing risk count and budgeted audit hours by taxonomies such as Information Technology, Finance, Research, Auxiliary Services, etc., with specific values for each category.]

Rating Legend:
- Critical
- High
- Medium
- Low
Systemwide IT Critical/High Risk Count vs. Audit Hours by IT Process
5. **U. T. System: Discussion and appropriate action regarding request for additional funding of $18,500,000 including $8,500,000 from Available University Funds (AUF) and $10,000,000 from Permanent University Fund (PUF) Bond Proceeds to fund Systemwide strategic security services provided by U. T. Austin and to conduct periodic assessments and exercises at the institutions for the period Fiscal Year 2024 - Fiscal Year 2028**

**RECOMMENDATION**

The Chancellor concurs in the recommendation of the Chief Compliance and Risk Officer, the Executive Vice Chancellor for Business Affairs, and the Vice Chancellor and General Counsel that the U. T. System Board of Regents approve additional funding in the amount of $18,500,000 including $8,500,000 from Available University Funds (AUF) and $10,000,000 from Permanent University Fund (PUF) Bond Proceeds for Systemwide security services and assessments at the institutions for Fiscal Year 2024 through Fiscal Year 2028.

It is also requested that within the total allocation of $18,500,000, the Executive Vice Chancellor for Business Affairs is authorized to adjust the individual allocations of AUF versus PUF Bond Proceeds to the extent necessary to optimize funding sources and to ensure that expenditures from PUF Bond Proceeds meet the requirements of Article VII, Section 18 of the Texas Constitution.

In addition, the Board is asked to find that expenditure of AUF for this purpose is appropriate under the U. T. System's responsibilities to oversee and coordinate the activities and operations of the U. T. institutions, with the intent that the expenditure will benefit all academic and health institutions and U. T. System Administration.

**BACKGROUND INFORMATION**

Information security is a significant high-risk area within the U. T. System. The Systemwide security services provided by U. T. Austin have reliably served U. T. institutions in detecting and reporting system compromises, high-risk vulnerabilities, and collecting useful data for forensics. Of the requested $18,500,000, $17,000,000 is expected to be used to upgrade the software and hardware used for the services and fund related staff at U. T. Austin and $1,500,000 is expected to be allocated for ongoing exercises and assessments at U. T. institutions.

U. T. Austin, System Administration, and institutions work together to enhance the strategic security services: vulnerability scanning, intrusion detection, and compilation of forensic log data. In Fiscal Year 2021, the intrusion detection component found more than thirty different types of malware across the System. Alerts are sent twenty four hours a day, three hundred sixty five days a year to security and information technology staff at each institution. The Board has funded these services since 2009. Of the $15,500,000 allocated by the Board in Fiscal Year 2018 to fund these services through Fiscal Year 2023, $14,344,866 has been expended.

Additional background information is provided in the PowerPoint on the following pages.
Strategic Security Services

Cam Beasley, Chief Information Security Officer, U. T. Austin
Helen Mohrmann, Chief Information Security Officer, U. T. System

U. T. System Board of Regents Meeting
Audit, Compliance, and Risk Management Committee
August 2022
Strategic Security Services Assist in Every Phase of an Attack

**PROACTIVE DEFENSE**
- **Vulnerability Scanning**
  - Identify Vulnerabilities

**STEPS IN AN ATTACK**
- **Reconnaissance**
  - An organization is targeted. Outward facing systems are scanned for vulnerabilities.
- **Malware Installation**
  - Vulnerabilities in systems are exploited - malware is deployed
- **Command & Control**
  - Attackers gain access and take control of system or network.
- **Lateral Movement**
  - Attackers move laterally within the network, spreading malware as they go.
- **Attempt Objective**
  - Exfiltrate data, launch ransomware, or disrupt business operations.

**ANALYSIS OF AN ATTACK**
- **Intrusion Detection**
  - Identify Compromised Systems • Find Malware • Detect Lateral Movement • Detect Data Exfiltration
- **Digital Forensic Analysis**
  - Analyze available Information: what is the source, how far has it spread, which accounts have been used?
Benefits to U. T. Institutions

- Identifies vulnerabilities and detects intrusions
- Leverages scarce expertise available at U. T. Austin
- Saves time and reduces cost to the institutions
- Identifies trends
Benefits to U. T. Austin

- Provides enriched environment for U. T. Austin’s information security team, funds some staff, improves retention
- Provides an applied cybersecurity learning environment for students
- Creates a unique, large store of data for use by cybersecurity researchers
Benefits to U. T. System

- Develops expertise in house instead of using third party vendors
- Reduces overall cost
- Ensures adequate coverage across System
- Provides a basis for metrics across System
- Supports System Administration’s fiduciary role
Exercises and Assessments with the Institutions

- FY19-22
  - Red Team simulated attacks
  - Incident response plan reviews
  - Ransomware tabletop
  - Phishing simulation

- FY22-23
  - Analysis of key controls coverage
  - Directory analysis
  - Metrics and Key Indicators development
  - Continued use of third party scoring system