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

Committee Meeting: 8/19/2020

Board Meeting: 8/20/2020
Austin, Texas

David J. Beck, Chairman
Christina Melton Crain
Jodie Lee Jiles
Janiece Longoria
Nolan Perez
Rad Weaver

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

<u>RECOMMENDATION</u>

No Consent Agenda items are assigned for review by this Committee.

2. **U. T. System: Discussion of Systemwide internal audit activities, including update on results of the Systemwide Cancer Prevention and Research Institute of Texas (CPRIT) grants assurance work and status of Fiscal Year 2020 Annual Audit Plan**

Chief Audit Executive Peppers will report on the assurance work conducted on the Cancer Prevention and Research Institute of Texas (CPRIT) grants at U. T. institutions by external providers. Additionally, Mr. Peppers will provide an update on the Fiscal Year 2020 Annual Audit Plan status as of May 31, 2020. A summary of the CPRIT assurance work 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 2019 CPRIT grant activity for six U. T. institutions. Four other U. T. institutions engaged Weaver & Tidwell to perform agreed upon procedures of FY 2019 CPRIT grant activity.

3. **U. T. System: Approval of the U. T. Systemwide Annual Audit Plan for Fiscal Year 2021**

RECOMMENDATION

Chief Audit Executive Peppers recommends approval of the proposed Fiscal Year 2021 U. T. Systemwide Annual Audit Plan (Audit Plan). 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 following pages. Additionally, the institutional 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.

The University of Texas System
Systemwide Internal Audit Program
Fiscal Year 2021 Annual Audit Plan Executive Summary

Systemwide Annual Audit Plan

The University of Texas (U. T.) Systemwide Fiscal Year (FY) 2021 Annual Audit Plan (Audit Plan) outlines the internal audit activities that will be performed by internal audit throughout the System in FY 2021. To provide consistency at the Systemwide level, the U. T. System Audit Office provided the institutional Chief Audit Executives (CAEs) with guidance in the spring of 2020 on the audit plan format, content, and development methodology, including the risk assessment process that supports the engagements selected to be on the individual audit plans, which were prepared in June and July 2020. The institutions' management and internal audit committees, as well as the U. T. System Audit Office and the Offices of Academic and Health Affairs, provided direction, input, and feedback on the audit plans. After the review process, each institutional internal audit committee formally approved its audit plan. The FY 2021 Audit Plan, as summarized in the tables and graphs that follow, is formally presented to the U. T. System Board of Regents for consideration for approval at the August 2020 meeting.

The methodology for audit plan development is designed to focus on the organization's strategic priorities and important objectives, identify related risks that could impede reaching them successfully, and develop engagements that provide validation that there are activities in place to mitigate the highest risks. Internal audit at each institution and System Administration conduct a risk assessment in which risks related to institutional priorities and objectives were identified and scored as Critical, High, Medium,

Risk Scoring Matrix		Impact		
		High	Medium	Low
Probability	High	C	H	M
	Medium	H	M	L
	Low	M	L	L

or Low. The Risk Scoring Matrix table (right) illustrates how the risks for each objective are scored based on the Probability rating of the risk occurring in the current environment and the Impact rating to the institution if the risk is realized. As Information Technology (IT) risks are the most prevalent across the System, additional focus is placed on IT risks through collaboration with IT and Information Security (IS) leadership to identify and agree upon critical services and functions that could have a significant impact on business objectives. In addition, internal audit purposefully considered the impact of risks in the context of operational changes due to COVID-19.

The engagements selected to be on the FY 2021 Audit Plan are derived directly from the risk assessment results, primarily addressing Critical and High risks, and also include other required and recurring work, as required by policy, statute, contract, or an external entity. For the Critical and High risks that are not addressed by the engagements, risk mitigation activities are identified and presented as part of the audit plan. These may include active monitoring work performed by other risk functions, executive support in the area, past year audit coverage, or review by an external party.

The following table lists the FY 2021 Audit Plan total budgeted audit hours by institution. These hours include engagements conducted by approximately 106 internal audit professional FTEs and co-source resources who are experts in selected audit areas that work with internal audit on engagements. However, with potential changes in priorities and staffing resources that may occur during the fiscal year, institutions may request approval from their respective presidents and/or internal audit committees to change their budgeted hours or reallocate budgeted hours among engagements and projects.

Institution	Budgeted Audit Hours
U. T. Arlington	9,966
U. T. Austin[1]	20,000
U. T. Dallas	11,240
U. T. El Paso	10,855
U. T. Permian Basin	4,680
U. T. Rio Grande Valley	9,990
U. T. San Antonio	8,880
U. T. Tyler	4,490
U. T. Southwestern Medical Center	19,540
U. T. Medical Branch - Galveston	11,030
U. T. Health Science Center - Houston	13,924
U. T. Health Science Center - San Antonio	8,321
U. T. M. D. Anderson Cancer Center	18,173
U. T. Health Science Center - Tyler	4,425
U. T. System Administration	14,495
Total Budgeted Audit Hours	**170,009**

While still staying vigilant of significant risks, the FY 2021 Audit Plan includes more consulting hours to serve in an advisory capacity and reserve hours for plan flexibility to be sensitive of the rapidly changing COVID-19 environment. The Audit Plan directs internal audit resources in three main sections: Engagements (Assurance Engagements, Advisory and Consulting Engagements, Investigations, and Follow-Up procedures); Development – Operations (ongoing operational activities); and Development – Initiatives and Education (developmental activities and continued education). Additionally, hours are set aside in a general reserve for unanticipated changes in resources and projects prompted by unexpected issues that may arise during the fiscal year. The table below depicts the percentage of budgeted audit hours allocated in these categories across the System.

Audit Plan Category	Budgeted Audit Hours	Percent
Assurance Engagements	67,717	40%
Advisory & Consulting Engagements	29,172	17%
Required Engagements	8,840	5%
Investigations	9,095	5%
Reserve	8,544	5%
Follow-Up	5,755	4%
Development – Operations	25,815	15%
Development – Initiatives & Education	15,071	9%
Total Budgeted Audit Hours	**170,009**	**100%**

Systemwide Risk Assessment

The approach for the Systemwide internal audit risk assessment is to start at the top with an awareness of key strategic priorities and operational objectives, discussion of those with a variety of stakeholders, and identification and assessment of the most relevant risks to develop the Audit Plan. The process is standardized by using common terms (Taxonomy) and criteria (Risk Scoring Matrix), enabling further analysis. As done in the past, an emphasis is placed on collaboration with other functions that assess, handle, or manage risk.

---

[1] Historically, the System Audit Office has performed an audit of the U. T. Austin Geology Foundation's management of the oil and gas interests and royalty payments received from the bequest of the John A. and Katherine G. Jackson's estate (Jackson Estate) every three years based on a condition in the waiver by the UT System Board of Regents of Regents' Rule 70301. After discussion among the System Audit Office, the Office of the Board of Regents, the UT Austin Office of Internal Audits, and the UT Austin Jackson School of Geosciences, it was agreed that the "periodic" audit of the Jackson Estate be transitioned to the UT Austin Office of Internal Audits, which would be conducted based on risk.

Approximately 2,400 risks were identified across the institutions and U. T. System Administration. The following Taxonomy areas had the highest numbers of total risks and the most Critical and High risks.

Academic Institutions:
- IT (see additional information on the following pages)
- Research – research administration, including pre- and post-award grant processes, conflicts of interest, and other compliance requirements; foreign influence; and export controls
- Auxiliary Services – Title IX; athletics; campus health and safety; and student housing
- Finance – financial reporting; budget alignment; tuition and revenue management; and CARES
- Enrollment management – student recruitment and admissions; financial aid processes

Health Institutions:
- IT (see additional information on the following pages)
- Governance – strategies; enterprise risk management; business continuity; and compliance program
- Patient care – delivering quality care; patient safety; medical staffing management; and credentialing
- Research – research administration and compliance, including pre- and post-award grant processes and other compliance requirements; foreign influence; and clinical trials
- Revenue cycle – process from admission to coding charges to billing

System Administration:
- IT – cybersecurity incident detection and response; use of third-party cloud services; data classification and asset management; and delivery of shared systems and infrastructure.
- Governance – Business continuity planning; investment compliance; strategic planning alignment with the U. T. System mission and related organizational change management
- Human Resources – succession planning and cross training; compensation, employee programs, and diversity and inclusion activities to recruit, develop, and retain employees
- Finance – account reconciliations/separation of duties

The following graph depicts the Systemwide count of risks, broken down by Risk Score, in the 22 Taxonomy areas. This is compared against the allocation of budgeted hours for engagements.
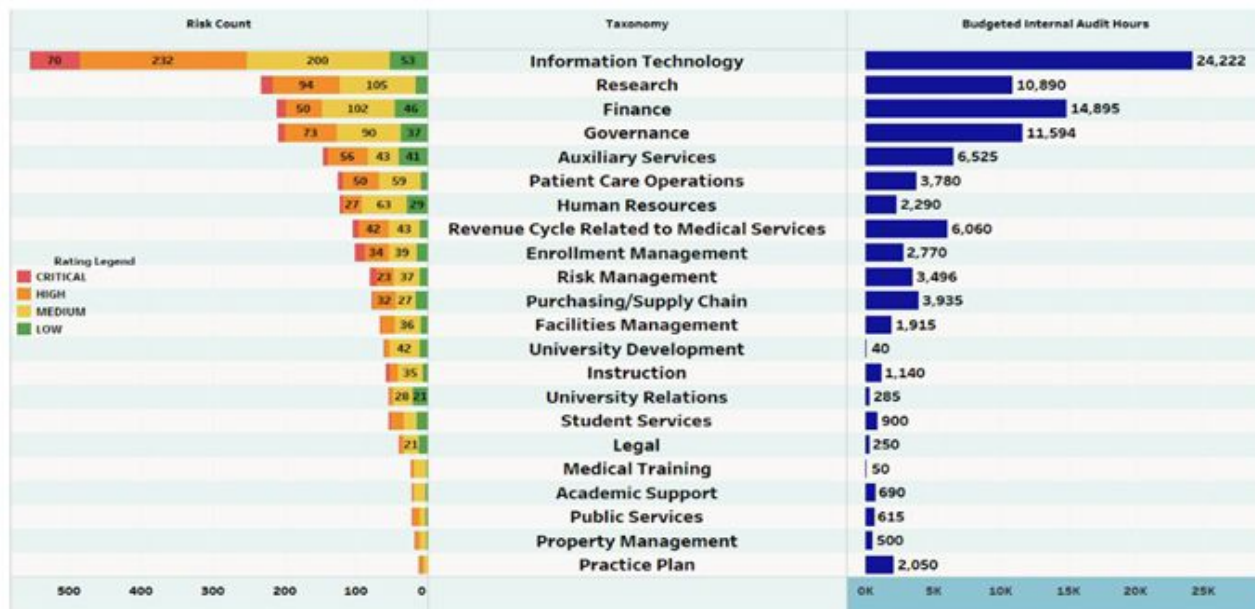
NOTE: Total audit hours in the graph are less than total budgeted hours noted on the previous page because engagements not associated with a Taxonomy are excluded (e.g., Investigations, Reserve, Follow-Up, and Development hours).

Systemwide IT Risk Assessment Methodology

During FY 2018, the System Audit Office initiated a project to develop an IT risk assessment methodology to assist internal audit at each institution and System Administration to consistently identify the most significant IT risks for an effective IT audit plan. As part of this process, a uniform framework was developed for defining IT areas (Domains) and functions (Processes), which provides a common language and organization for collaboration and comparison among U. T. institutions.

The common framework also facilitates the identification of cross-institution risks and trends. Data Stewardship, Ownership and Governance was the most frequently identified Critical or High risk area, with 13 institutions and System Administration citing at least one Critical or High risk in these areas. The most common Critical and High-risk areas identified during this year's risk assessment are:
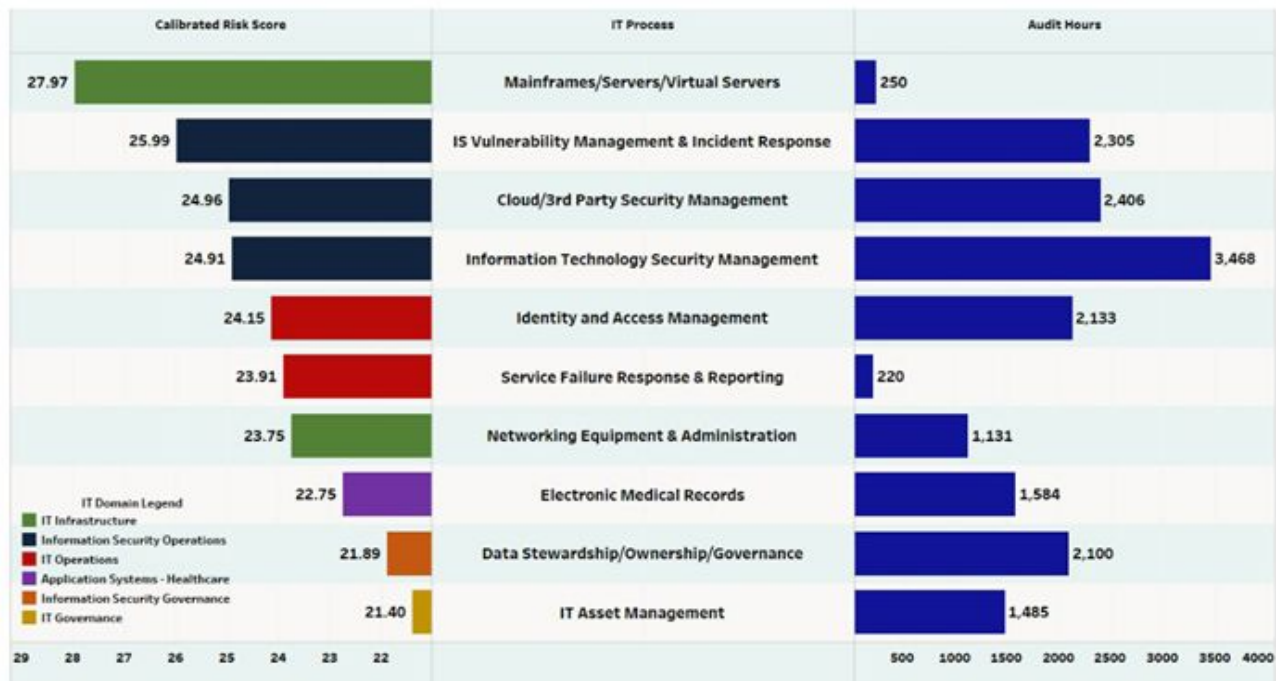
IT Process	# of Institutions*
Data Stewardship/Ownership/Governance	13
IS Vulnerability Management & Incident Response	12
Disaster Recovery/Business Continuity/Emergency Preparedness	11
Cloud/Third-Party Security Management	10
Mobile Devices & Portable Data Storage	10
Server & Desktop Configuration Management	9
Identity and Access Management	8
IT Asset Management	8
Oversight of Decentralized IT Operations	8

* Includes UT System Administration where applicable.

The methodology also improves visibility into U. T. System risk through Calibrated Risk Scores (CRS), which are numeric values calculated based on risk ratings (Critical, High, Medium, Low) with weighting applied based on institution and Domain/Process factors. This results in the ability to prioritize the full inventory of IT risks, such that Critical and High risks are ranked by their significance to U. T. System as a whole, which can be used for internal audit resource allocation. The weighting of the CRS is based on institutional calibration factors (including multi-institution or Systemwide; academic or health; budget; research expenditures; faculty and staff headcounts; and enrollment) and process calibration (relative risk among processes -- e.g., cybersecurity incident response is weighted higher than IT project management).

The top ten U. T. System IT risk areas based on CRS of Critical and High risks compared against the allocation of budgeted hours for engagements are displayed below:

Calibrated Risk Score	IT Process	Audit Hours
27.97	Mainframes/Servers/Virtual Servers	250
25.99	IS Vulnerability Management & Incident Response	2,305
24.96	Cloud/3rd Party Security Management	2,406
24.91	Information Technology Security Management	3,468
24.15	Identity and Access Management	2,133
23.91	Service Failure Response & Reporting	220
23.75	Networking Equipment & Administration	1,131
22.75	Electronic Medical Records	1,584
21.89	Data Stewardship/Ownership/Governance	2,100
21.40	IT Asset Management	1,485

IT Domain Legend
- IT Infrastructure
- Information Security Operations
- IT Operations
- Application Systems - Healthcare
- Information Security Governance
- IT Governance

The graph below depicts the Critical and High risks covered by the FY 2021 and prior year Audit Plans:

Included in FY21 Audit Plan (49%)
Included in Prior Year Audit Plan (22%)
Not Covered (29%)

	IT Leadership & Governance	IT Operations	Information Security Governance	Information Security Operations	IT Infrastructure	Application Systems - Business Operations	Application Systems - Healthcare	Application Systems - Research	Application Systems - Academic
# of Critical and High Risks:	47	63	41	88	26	10	18	7	2