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

Committee Meeting: 8/14/2019

Board Meeting: 8/15/2019
Austin, Texas

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

	Committee Meeting	Board Meeting	Page
4. **U. T. System: Report and discussion on Information Security Program**	*10:20 a.m.* **Report/Discussion** *Ms. Mohrmann*	Not on Agenda	**40**
D. ADJOURN	*10:30 a.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 6 and 7.

2. U. T. System: Approval of the U. T. Systemwide Annual Audit Plan for Fiscal Year 2020 and update on status of Fiscal Year 2019 Annual Audit Plan

RECOMMENDATION

Chief Audit Executive Peppers recommends approval of the proposed Fiscal Year 2020 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 members of the Audit, Compliance, and Risk Management Committee (ACRMC) prior to the meeting.

Additionally, Mr. Peppers will provide an update on the Fiscal Year 2019 Annual Audit Plan status as of May 31, 2019. Details on the plan status were provided to the ACRMC 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 2020 Annual Audit Plan Executive Summary

Systemwide Annual Audit Plan

The University of Texas (U. T.) Systemwide Fiscal Year (FY) 2020 Annual Audit Plan (Audit Plan) outlines the internal audit activities that will be performed by internal audit throughout the System in FY 2020. 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 2019 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 2019. 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 2020 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 2019 meeting.

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

The audit plans are prepared using a risk-based approach to ensure that areas and activities with the greatest risk are identified for consideration to be audited. Internal audit at each institution and System Administration conduct a risk assessment in which risks related to important institutional objectives were identified and rated as Critical, High, Medium, or Low. The Risk Scoring Matrix table (right) illustrates how the risks for each objective are scored based on the Probability of the risk occurring in the current environment and the Impact 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, for FY 2020, internal audit purposefully considered risks in the areas of intellectual property and construction (for those institutions now managing their own capital projects).

The engagements selected to be on the FY 2020 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 monitoring work performed by other risk functions, past year audit coverage, or review by an external party.

The following table lists the FY 2020 Audit Plan total budgeted audit hours by institution. These hours include engagements conducted by approximately 116 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.

Consolidation Prepared by: U. T. System Audit Office
Date: July 2019

Institution	Budgeted Audit Hours
U. T. Arlington	10,140
U. T. Austin	19,200
U. T. Dallas	14,862
U. T. El Paso	10,145
U. T. Permian Basin	4,685
U. T. Rio Grande Valley	9,417
U. T. San Antonio	10,300
U. T. Tyler	4,490
U. T. Southwestern Medical Center	19,690
U. T. Medical Branch - Galveston	11,822
U. T. Health Science Center - Houston	14,212
U. T. Health Science Center - San Antonio	8,827
U. T. M. D. Anderson Cancer Center	21,250
U. T. Health Science Center - Tyler	4,315
U. T. System Administration	15,725
Total Budgeted Audit Hours	**179,080**

The FY 2020 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	69,167	39%
Advisory & Consulting Engagements	26,945	15%
Required Engagements	15,300	9%
Investigations	9,360	5%
Reserve	8,485	5%
Follow-Up	5,855	3%
Development – Operations	27,222	15%
Development – Initiatives & Education	16,746	9%
Total Budgeted Audit Hours	**179,080**	**100%**

Systemwide Risk Assessment

As part of the FY 2020 Audit Plan process, the institutional and System Administration internal auditors executed a strategic and operational objective-based risk assessment. The goal for this common risk assessment approach was to start at the top with an awareness of critical objectives and discussion with key stakeholders to ensure the risks assessed by the Audit Plan were the most relevant. The assessment process was standardized by using common terms (Taxonomy) and criteria (Risk Scoring Matrix), enabling further analysis. As done in the past, an emphasis was placed on collaboration with other functions that assess, handle, or manage risk.

Consolidation Prepared by: U. T. System Audit Office
Date: July 2019

Approximately 2,335 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 within compliance and biosafety requirements; intellectual property protection; and export controls
- Auxiliary Services – Title IX; athletics compliance; campus safety; and student housing
- Finance – financial reporting; budget alignment; accounts payable; and payroll
- Enrollment management – student recruitment and admissions/financial aid processes

Health Institutions:

- IT (see additional information on the following pages)
- Governance – strategies; structures; partners; business continuity; and compliance program
- Research – research administration and compliance; pre and post award processes; faculty and institutes; and intellectual property protection
- Patient care – delivering quality care; patient safety; staffing management; and credentialing
- Revenue cycle – process from admission to coding charges to billing

System Administration:

- IT – cybersecurity vulnerability management and incident response; data stewardship and governance; funding; and access management
- Governance – strategic planning; resource stewardship; role in supporting institutional needs; succession planning and cross training; and managing organization change
- Finance – strategic financial planning/budgeting and 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: The 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).

Consolidation Prepared by: U. T. System Audit Office
Date: July 2019

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. Cybersecurity Vulnerability Management and Incident Response, and Data Stewardship, Ownership and Governance, were the most frequently identified Critical or High risk areas, 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:

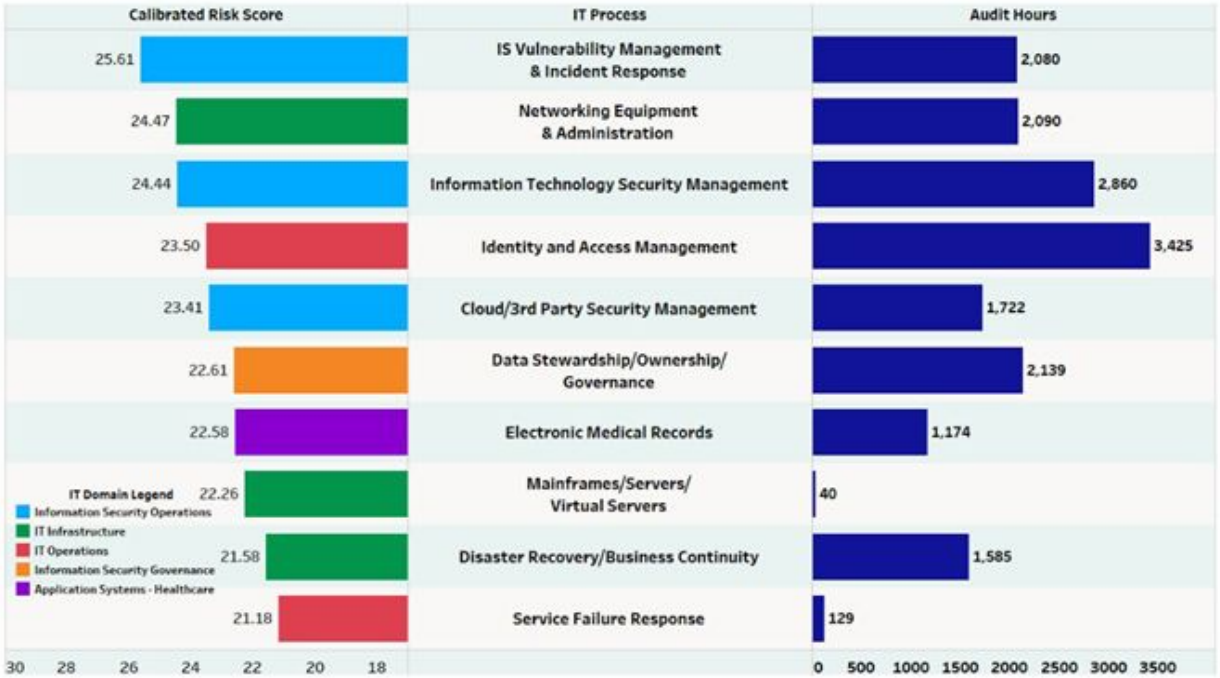
IT Process	# of Institutions*
Cybersecurity Vulnerability Management & Incident Response	14
Data Stewardship/Ownership/Governance	14
Mobile Devices & Portable Data Storage	13
IT Asset Management	12
Identity & Access Management	11
Networking Equipment & Administration	11
Cloud/Third-Party Security Management	11

** Includes UT System Administration where applicable.*

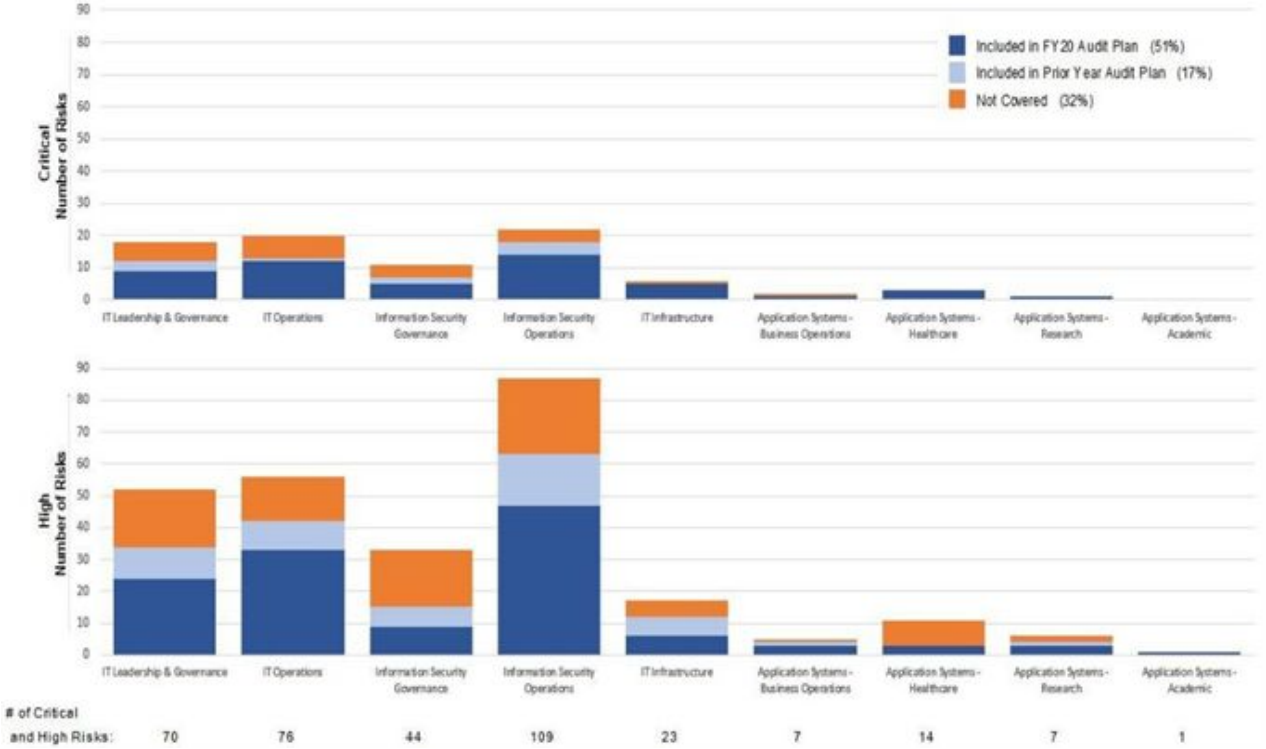
The methodology also improves visibility into U. T. System risk through Calibrated Risk Scores (CRS), which are numeric values calculated based on risk ratings (Critical, High, Medium, Low) with weighting applied based on institution and Domain/Process factors. This results in the ability to prioritize 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).

Consolidation Prepared by: U. T. System Audit Office
Date: July 2019

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:



The graph below depicts the Critical and High risks covered by the FY 2020 and prior year Audit Plans:



Consolidation Prepared by: U. T. System Audit Office
Date: July 2019

3. U. T. System Board of Regents: Discussion and appropriate action regarding proposed amendments to Regents' *Rules and Regulations*, Rule 20402 (Provision of Audit and Non-Audit Services by External Audit Firms), regarding the definition of Audit Services

RECOMMENDATION

The Chancellor concurs in the recommendation of the Executive Vice Chancellor for Academic Affairs, the Executive Vice Chancellor for Health Affairs *ad interim*, the Executive Vice Chancellor for Business Affairs, the Vice Chancellor and General Counsel, and the Chief Audit Executive that Regents' *Rules and Regulations*, Rule 20402 (Provision of Audit and Non-Audit Services by External Audit Firms), be amended as set forth below in congressional style:

…

Audit Services - ~~are~~ services ~~provided for the purpose of expressing an opinion on the financial statements of U. T. System or any of the institutions~~ that result in an audit, review, or agreed-upon procedures communication for U. T. System or any of the institutions.

….

BACKGROUND INFORMATION

Regents' Rule 20402 regulates the provision of audit and non-audit services by external audit firms to U. T. System Administration and U. T. institutions. Under the Rule, any engagement of an external audit firm for services outside the definition of "audit services" must be approved by the Audit, Compliance, and Risk Management Committee (ACRMC) to assure that no conflict of interest is created by the proposed engagement.

Audit services are currently defined as "services provided for the purpose of expressing an opinion on the financial statements." However, in industry practice, audit services can also include review of financial information other than an organization's financial statements and review of non-financial aspects of an organization. The proposed amendment broadens this definition to allow U. T. System to obtain other limited types of audit services such as program audits, financial reviews for accreditation, or agreed upon procedures without approval by the ACRMC. These types of engagements would continue to be reviewed by multiple parties and result in a formal communication report and will also require delegation of audit authority from the State Auditor's Office.

These revisions do not impact the full-time equivalent (FTE) employee count Systemwide and have the potential for a slightly favorable budget impact through process simplification. The proposed amendments were reviewed by the institutional presidents and representatives of the Student Advisory Council, the Faculty Advisory Council, and the Employee Advisory Council.

4. U. T. System: Report and discussion on Information Security Program

REPORT

Ms. Helen Mohrmann, Chief Information Security Officer, will report on activities of the Office of Information Security and various initiatives. A PowerPoint presentation is set forth on the following pages.

BACKGROUND INFORMATION

The Office of Information Security oversees security for information systems managed by U. T. System Administration and provides a stewardship and service function to U. T. institutions. This Office also administers funds allocated by the Board for information security. This annual report will review use of those funds and current projects.

Information Security Annual Report

Ms. Helen Mohrmann, Chief Information Security Officer

U. T. System Board of Regents' Meeting
Audit, Compliance, and Risk Management Committee
August 2019

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.
WWW.UTSYSTEM.EDU

Information Security Risks to the U. T. Mission

- Interference with or loss of operations
- Theft or corruption of student, employee, or patient data
- Theft or corruption of intellectual property

Information Security Strategy Framework

Communicate	• Explain risk and mitigation strategies to stakeholders
Identify	• Know what assets we need to protect and their relative importance
Protect	• Take effective measures to protect our assets
Detect	• Quickly catch the threats we couldn't stop
Respond	• Prioritize and remediate incidents
Recover	• Promptly return to a good state of operations

Current U. T. System Projects and Services

	FY 19	FY 20
Communicate	Develop New Risk Report	Issue New Risk Report Revise Annual Report Template
Identify	Include Inventory in Risk Report	
Protect	Identify Gaps in Network Security	Address Gaps in Network Security Conduct Daily Vulnerability Scans
Detect	Re-design Intrusion Detection Service	Deploy Intrusion Detection Service Conduct Security Tests (Red Teams)
Respond		Conduct Incident Response Health Checks
Recover		

Provided by U. T. Austin under contract to U. T. System Administration

New Information Security Risk Report

- Rates eighteen categories of risks
- Discusses mitigation strategies
- Provides overview of mission-critical and high-risk assets
- Describes the level of decentralized asset management

Institution Network Security Assessment

- Established a baseline for network security
- Identified strengths and gaps at each institution
- Currently working with the institutions to develop remediation plans

Intrusion Detection Service

- Validated the design and cost estimates with a third party
- Developed a planning process to work with each institution
- First two institutions are implemented: U. T. Dallas, U. T. Southwestern Medical Center
- Two or three more institutions will be implemented before the November meeting

Information Security Strategy Implementation

- Leverage the expertise of the U. T. institutions
  - U. T. Austin provides several services to the institutions under contract from U. T. System
  - Recurring community conference calls on specific topics enable institutions to share information
  - CISOs meet quarterly
  - Bi-annual information security conference fosters networking among information technology and security professionals across institutions

Strategy Implementation continued

- Established institutional Information Security (IS) function that is separate from the central Information Technology (IT) organization
  - IT performs the front-line operational work of applying technical controls for systems managed by central IT
  - IS provides guidance and oversight to central and distributed IT organizations