The University of Texas Health Houston (UTHealth Houston)
Internal Audit Annual Report for 2025

Purpose of the Internal Audit Annual Report: To provide information on the assurance services, consulting services, and other activities of the internal audit function. In addition, the internal audit annual report assists oversight agencies in their planning and coordination efforts.

Table of Contents

Purpose of the Internal Audit Annual Report: To provide information on the assurance services, consulting services, and other activities of the internal audit function. In addition, the internal audit annual report assists oversight agencies in their planning and coordination efforts.

I. Compliance with Texas Government Code, Section 2102.015: Posting the Internal Audit Plan, Internal Audit Annual Report, and Other Audit Information on the website.

The Internal Audit Plan and Internal Audit Annual Report is contained within the Reports to the State section of UTHealth Houston's website as required by Texas Government Code, Section 2102.015. An updated report is provided to the web developer who then posts the information no later than one day prior to the due date for submission to the appropriate reporting state agencies.

II. Internal Audit Plan for Fiscal Year 2025

Audit Number	FY 2025 Audit Plan Audit / Project	Description	Status	Report Date
Assurance Engagements				
HSC25ASCF0001	CIM - Diagnostic & Interventional Imaging (carried forward)	Review the operational and financial controls of the McGovern Medical School, Department of Diagnostic, and Interventional Imaging.	Complete	1/30/2025
HSC25ASCF0002	Data Consortiums (carried forward)	Review governance controls around data consortiums where UTHealth Houston serves as custodian.	Complete	9/10/2024
HSC25ASCF0003	LabArchives (carried forward)	Review controls around the LabArchives application.	Complete	9/9/2024
HSC25ASCF0004	SaaS Backups (carried forward)	Review controls around Software-as-a-Service tool (Druva) for Teams/One Drive/Exchange Online backups.	Complete	11/4/2024
HSC25ASCF0005	Windows Server Patching (carried forward)	Review controls around Windows Server patching. Meets biannual assessment requirement for compliance with TAC 202.	Complete	6/2/2025
HSC25AS0001	AI Governance	Review controls over the use of externally available AI.	In Progress	
HSC25AS0002	UCT Data Center	Review controls over the UCT data center. *Also meets the biennial compliance requirement with Texas Administrative Code Section 202*.	Complete	9/8/2025
HSC25AS0003	DSRDP	Review compliance with DSRDP processes/bylaws based on assessed risk.	Complete	6/2/2025
HSC25AS0004	Emergency Management Plan	Review the adequacy of UTHH processes and policies developed to respond to emergency events	Complete	6/3/2025

HSC25AS0005	Epic Work Queues	Review controls around work queues in Epic.	Complete	5/28/2025
HSC25AS0006	Inbound Email Security	Review controls around the inbound email security solution (Abnormal).	In Progress	
HSC25AS0007	Medical Device Network Segmentation	Review controls around the segmentation of medical devices from the UTHH network.	Cancelled	IT Security is exploring a replacement Product. We will continue to monitor developments.
HSC25AS0008	MSRDP	Review compliance with MSRDP processes/bylaws based on assessed risk.	Cancelled	Epic Work Queues (HSC25AS0005) serves as the FY25 MSRDP audit.
HSC25AS0009	Research Security Program	Review controls associated with the research security program as required by National Security Presidential Memorandum 33 (NSPM-33) and TEC 51.956.	Cancelled	Federal government has not provided final guidance. We will continue to monitor developments.
HSC25AS0928	CIM-UTP	Review the operational and financial controls of UT Physicians.	In Progress	
HSC25AS1446	Research Service Center	To perform an operational review of the efficiency and effectiveness of the Research Service Center.	In Progress	
Required Engagements				
HSC25RQ0001	Epic Security Certification	Verify IT Security's control certification to Epic (annual requirement).	Complete	3/11/2025
HSC25RQ0002	External Auditor Assistance	Assist the State Auditor's Office and other external audit functions.	Complete	No report Issued
HSC25RQ0003	FY24 Financial Statements	Review controls over transactions and perform analytical reviews/other procedures assigned as part of the procedures for the FY24 financial statements.	Complete	Report issued by Deloitte at UT System level.
HSC25RQ0004	FY25 Financial Statements	Perform interim procedures for the FY25 financial statements.	Complete	Report issued by Deloitte at UT System level.
HSC25RQ0005	THECB	Provide an opinion on revenue and expenditures reporting on program funds.	Complete	12/19/2024
Follow-Up				
HSC25FL0001	Follow-Up	Hours designated to perform periodic follow-up to validate the status of implementing outstanding recommendations	Complete	9/1/2025

Compliance with Texas Education Code, Section 51.9337(h)

Senate Bill 20 (84th Legislative Session) made several modifications and additions to Texas Government Code (TGC) and Texas Education Code (TEC) related to purchasing and contracting. Effective September 1, 2015, TEC Section 51.9337(h) requires that, *"The chief auditor of an institution of higher education shall annually assess whether the institution has adopted the rules and policies required by this section and shall submit a report of findings to the state auditor."* UTHealth Houston's Auditing and Advisory Services conducted this required assessment for fiscal year 2025, and found the following:

Based on review of current institutional policy and the UT System Board of Regents' *Rules and Regulations*, UTHealth Houston has generally adopted all of the rules and policies required by TEC Section 51.9337. Review and revision of institutional and System policy is an ongoing process. These rules and policies will continue to be assessed annually to ensure continued compliance with TEC Section 51.9337.

III. Consulting Services and Other Activities

Report No.	Name of Project	High-Level Consulting Engagement / Non-audit Service Objective(s)	Observations / Results and Recommendations
HSC25ADCF0001	Development Operations Advisory (Carried forward)	Perform an analysis of Development and Public Affairs processes from an efficiency, effectiveness, and economy of operations perspective.	Results communicated to the department
HSC25ADCF0002	Medical Devices Advisory (Carried forward)	Review controls over medical devices are adequate and functioning as intended.	Results communicated to the department
HSC25AD0001	Data Analytics	Assisting departments with data analytics needs	Results communicated to the department
HSC25AD0005	TEC 51.3525	Assist management in ensuring compliance with TEC 51.3525.	Results communicated to the department
HSC25AD0019	Manual Patching Agreements Advisory	Review whether controls over manual patching agreements are adequate and functioning as intended.	Results communicated to the department
HSC25AD0757	Cloud Platform Security Advisory	Review whether controls over cloud platform security are adequate and functioning as intended.	Results communicated to the department
HSC25AD0758	Patient Record Releases Advisory	Review whether patient record releases are authorized and processed in accordance with institutional policy.	Results communicated to the department
HSC25AD0790	SoD Inventory Controls	Review to assess the controls over the handling and storage of nitrous oxide at the School of	Results communicated to the department

		Dentistry and the University Dental Center where the Advanced Education General Dentistry program is based.	
HSC25AD1062	IT Security Vendor Risk Assessment Advisory	Review whether controls for third party vendor risk assessments are adequate and functioning as intended.	In Progress
HSC25AD1441	Epic Payer Platform Advisory	Review whether security access controls around Epic Payer Platform are adequate and functioning as intended.	In Progress
HSC25AD1442	Medical Devices Advisory	Review controls over medical devices are adequate and functioning as intended.	Not completed since the department is performing their own monitoring process.

IV. External Audit Services

Service	Provider
Opinion on financial statements of UT Physicians (a component unit of The University of Texas System)	Blazek & Vetterling LLP Certified Public Accountants
Financial Statements FY 2024 Assurance Work	Deloitte and Touche LLP (Deloitte) Certified Public Accountants
Financial Statements FY 2025 Assurance Work	Deloitte and Touche LLP (Deloitte) Certified Public Accountants
Financial Portion of the Statewide Single Audit	State Auditor's Office
Cancer Prevention and Research Institute of Texas (CPRIT) Program	Deloitte and Touche LLP (Deloitte) Certified Public Accountants
Opinion on combined financial statements of UTHealth Houston Behavioral Sciences Campus (an operating unit of The University of Texas Health Science Center Houston) for FY 2024 and 2025	Forvis Mazars, LLP Certified Public Accountants

V. External Quality Assurance Review (Peer Review)

November 2023

Mr. Daniel Sherman, Vice President and Chief Audit Officer
The University of Texas Health Science Center at Houston

In June 2023, The University of Texas Health Science Center at Houston (UTHealth Houston) internal audit (IA) function, Auditing & Advisory Services (A&AS), completed a self-assessment of internal audit activities in accordance with guidelines published by the Institute of Internal Auditors (IIA) for the performance of a quality assessment review (QAR). UTHealth Houston A&AS engaged an independent review team consisting of internal audit professionals with extensive higher education and healthcare experience to perform an independent validation of A&AS' QAR self-assessment. The primary objective of the validation was to verify the assertions made in the QAR report concerning A&AS' conformity to the IIA's International Standards for the Professional Practice of Internal Auditing (the IIA Standards) and Code of Ethics, Generally Accepted Government Auditing Standards (GAGAS), and the relevant requirements of the Texas Internal Auditing Act (TIAA).

The IIA's *Quality Assessment Manual* suggests a scale of three ratings, "Generally Conforms," "Partially Conforms," and "Does not Conform." "Generally Conforms" is the top rating and means that an internal audit activity has a charter, policies, and processes that are judged to be in conformance with the *Standards*. "Partially Conforms" means deficiencies in practice are noted that are judged to deviate from the *Standards*, but these deficiencies did not preclude the A&AS activity from performing its responsibilities in an acceptable manner. "Does not Conform" means deficiencies are judged to be so significant as to seriously impair or preclude the A&AS activity from performing adequately in all or in significant areas of its responsibilities.

Based on our independent validation of the QAR performed by A&AS, we agree with A&AS' overall conclusion that the internal audit function **"Generally Conforms"** with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and Code of Ethics, as well as with A&AS' conclusions regarding GAGAS and TIAA requirements. Our review noted strengths as well as opportunities for enhancing the internal audit function.

This information has been prepared pursuant to a client relationship exclusively with, and solely for the use and benefit of, The University of Texas System Administration and UTHealth Houston and is subject to the terms and conditions of our related contract. Baker Tilly disclaims any contractual or other responsibility to others based on its use and, accordingly, this information may not be relied upon by anyone other than The University of Texas System Administration and The University of Texas Health Science Center at Houston.

The review team appreciates the cooperation, time, and candid feedback of executive leadership, stakeholders, and A&AS personnel.

Very truly yours,

Baker Tilly US, LLP

Baker Tilly US, LLP

VI. Internal Audit Plan for Fiscal Year 2026

FY 2026 Audit Plan Audit / Project	Budgeted Hours	Description
Assurance Engagements		
MSRDP	400	Review compliance with MSRDP processes/bylaws based on assessed risk.
DSRDP	400	Review compliance with DSRDP processes/bylaws based on assessed risk.
Review & Validation	150	Review controls around review & validation requirements per UTS 142 Financial Accounting and Reporting.
Hard Drive Decommissioning	450	Review controls around hard drive decommissioning.
Restricted Patient Records	500	Review controls around Epic's Break the Glass feature.
Physician Revenue	550	Review controls around physician revenue.
System Owner Program	450	Review controls around the system owner program employed by IT Security.
Unstructured Data Storage	550	Review controls around unstructured data storage (Isilon Storage System). Serves as TAC 202 engagement.
Epic Interfaces	550	Review controls around interfaces to/from Epic.
Web Accessibility	500	Review controls/compliance with web accessibility standards.
Carryforward	800	Carryforward of prior year engagements.
Assurance Engagements Subtotal	**5,300**	
Required Engagements		
FY25 Financial Statements	90	Review controls over transactions and perform analytical reviews/other procedures assigned as part of the procedures for the FY25 financial statements.
FY26 Financial Statements	60	Perform interim procedures for the FY26 financial statements.
External Auditor Assistance	200	Assist the State Auditor's Office and other external audit functions.
Epic Security Certification	300	Verify IT Security's control certification to Epic (annual requirement).
Required Engagements Subtotal	**650**	
Advisory Engagements		
UTHH Committees	300	Attend UTHH committees to monitor business developments.
Financial Advisory	600	Assist management in reviewing financial controls.
Data Analytics	300	Assist management using data analytics.
TEC 51.3525	300	Assist management in ensuring compliance with TEC 51.3525.
Management Assistance	100	Assist management with requests.
IT Advisory	800	Assist management in reviewing information technology controls.
Advisory Engagements Subtotal	**2,400**	
Reserve		
Assurance/Advisory Reserve	1,000	Perform assurance/advisory engagements requested by management.

Reserve Subtotal	**1,000**	
Investigations		
Investigations	300	Review thefts or assist in other risk management functions.
Triage	100	Perform procedures related to compliance intakes or assist other risk management functions.
Investigations Subtotal	**400**	
Follow-up		
Follow-up	500	Perform periodic follow-up to validate the status of implementing outstanding recommendations.
Follow-up Subtotal	**500**	
Operations		
External Assistance/Requests	100	Provide assistance to UT System and other external agencies. Includes reporting, processing information requests, and other assistance including reviewing for compliance with TEC 51.9337 Purchasing Authority Required Standards.
Internal Process Improvement	400	Review/update of A&AS audit processes.
Internal Audit Committee	500	Prepare Internal Audit Committee packages and related post-meeting documentation.
FY 2027 Audit Plan	400	Developing annual audit plan using risk assessment techniques as required by Government Code 2102.
Internal Audit Annual Report	50	Preparation and Posting of the Internal Audit Plan, Internal Audit Annual Report, and other information required by TGC 2101.015.
Staff Meetings	500	Participate in departmental staff meetings.
eCase/IDEA	300	Train, develop, and perform maintenance associated with eCase/IDEA.
Quality Assessment Review	200	Evaluate departmental processes in preparation for the next external quality assessment review (QAR). Yellow Book standards require a QAR every three years.
Operations Subtotal	**2,450**	
Initiatives and Education		
Professional Activities	63	Writing, publication, external presentations, and participation in professional organizations.
UT System Initiatives	200	Participation in UT System initiatives including committees, workgroups, etc.
CPE/Training	400	Professional training and CPE courses to keep certifications active.
Initiatives and Education	**663**	
Total Budgeted Hours	**13,363**	

High Risks Not Included in FY 2026 Audit Plan	Explanation / Mitigation	Internal Audit Action
Risk financial counselors do not understand the correct way to handle patient credit balances resulting in excessive amount of payments being unapplied.	Monitor Developments	Monitor Developments
Inadequate coordination of data analytic efforts resulting in inefficiencies and inconsistent results.	Monitor Developments	Monitor Developments

HUB expansion is not adequately planned/reviewed resulting in increased costs.	Monitor Developments	Monitor Developments
Capital investments to fund IT infrastructure/AI needs are not available resulting in financial losses.	Monitor Developments	Monitor Developments
Inability to accurately plan, forecast, and develop enterprise risk management for federal funding cuts for research and patient care activities that could affect resource allocation may result in operational inefficiencies, including loss of key research and patient care faculty, discontinuation of important research projects, and decline in the quality of patient care.	Monitor Developments	Monitor Developments
Growth of the healthcare practice resulting in increased Epic costs.	Monitor Developments	Monitor Developments
Immigration sponsorship processes are not in compliance with federal/state/local regulations resulting in operational inefficiencies.	Monitor Developments	Monitor Developments
Contracts are not awarded and managed in compliance with relevant laws, rules, and policies (TEC 51.9337)	Monitor Developments	Monitor Developments
Delays in physician credentialing resulting in billing delays and financial losses.	Covered by external consulting firm	Monitor Developments
Inability to expand clinical practice due to availability of space/funding resulting in lost revenue.	Monitor Developments	Monitor Developments
Change in management leads to reduced controls/oversight and/or operational inefficiencies.	Covered by FY25 CIM-UTP; Monitor Developments	Monitor Developments
Inability to recruit candidates to fill open healthcare positions resulting in lost revenue and operational inefficiencies.	Monitor Developments	Monitor Developments
Loss of key employees with no succession planning resulting in lost revenue and operational inefficiencies.	Monitor Developments	Monitor Developments
TIPS reporting methodology presents ongoing issues and uncertainty resulting in future lost funding and/or contract violations.	Monitor Developments	Monitor Developments
ASC ownership and other expansion efforts resulting in a damaged relationship with hospital partner.	Monitor Developments	Monitor Developments
Relationship/financial dependence on MH resulting in limitation of growth potential.	Monitor Developments	Monitor Developments
Different processes between UTHH and UTP resulting in inefficiencies	Monitor Developments	Monitor Developments
Absence of clear policies, training, and human oversight of AI use could lead to ethical, legal, reputational, or academic integrity concerns.	Covered by FY25 AI Governance	In Progress
Payers with access to patient records through the Epic Payer Platform access more than the minimum necessary information to deny more claims resulting in a breach.	Covered by FY25 Patient Record Access Advisory	Report Submitted

Patches/upgrades are not applied timely resulting in a breach.	Covered by FY25 Windows Server Patching/FY25 Manual Patching Agreements Advisory	Report Submitted
Breach in data consortiums with UTHH as custodian resulting in financial costs and reputational damage.	Covered by FY24 Data Consortiums	Report Submitted
Hacker compromises research/medical devices and penetrates network resulting in a breach.	Monitor Developments	Monitor Developments
Phishing attacks are successful resulting in a breach.	Covered by FY25 Inbound Email Security	In Progress
Data center may not have appropriate safeguard and security controls in place resulting in a breach or business disruption	Covered by FY25 Data Center Operations	Report Submitted
Researchers lose IP while traveling to foreign countries resulting in financial losses.	Monitor Developments	Monitor Developments
Security assessments not performed for changes to applications containing sensitive data resulting in a breach.	Covered by FY25 IT Security Vendor Risk Assessment Advisory	In Progress
Security risk assessments of software/ applications procured through Coupa are not performed prior to implementation resulting in a breach.	Covered by FY25 IT Security Vendor Risk Assessment Advisory	In Progress
UTHealth is not in compliance with NSPM 33 Research Security Program resulting in fines and other penalties.	Monitor Developments	Monitor Developments
Use of AI in adding information to a patient record is not validated by the provider resulting in inaccurate patient records.	Covered by FY25 AI Governance	In Progress
Controls over controlled substances/drugs are not adequate resulting in theft and reputational damage.	Covered by UT Police Incident reports	Monitor Developments
Inadequate infrastructure in managing clinical trials resulting in decreased funding.	Monitor Developments	Monitor Developments
Shortage of qualified research coordinators resulting in inability to manage grants	Monitor Developments	Monitor Developments
Research projects partially funded by foreign influence resulting in loss of intellectual property	Monitor Developments	Monitor Developments

Our risk assessment methodology included interviews and questionnaires to update the annual risk assessment. The identified risks were organized into institution-wide areas such as financial management, human resources management, and purchasing/warehousing. We developed detailed risk assessments of high-risk areas of research, information technology, and patient care. For each identified risk, probability and impact were determined using three to seven factors such as regulatory environment and frequency of identification in responses for the financial/operational risks and scope of process and age of system for the IT risks.

Compliance with Texas General Appropriations Act, Benefits Proportionality Audit Requirement for Higher Education Institutions

Rider 8, page III-58, the General Appropriations Act (89th Texas Legislature) requires the folllowing:

a. For fiscal year 2026 and 2027, institutions of higher education shall also consider audits of benefits proportionality when developing their annual internal audit plans.

b. It is the intent of the Legislature that the State Auditor's Office audit at least two institutions of higher education for compliance with benefits proportional provisions during the 2026-27 biennium.

c. If an audit conducted under Subsections (a) and (b) identifies any instances in which an institution has not been compliant with the proportionality requirements provided in Article IX, Section 6.08, Benefits Paid Proportional by Method of Finance and received excess monies from the General Revenue Fund as a result of this noncompliance, the institution shall submit a reimbursement payment to the Comptroller of Public Accounts within two years from the conclusion from the audit. The Comptroller of Public Accounts shall notify the Legislative Budget Board and State Auditor's Office of all reimbursement payments submitted by an institution of higher education.

Benefits proportionality was considered during the FY 2026 annual risk assessment. It was not assessed as a high risk and therefore not included in the FY 2026 Audit Plan.

VII. Reporting Suspected Fraud and Abuse

UTHealth Houston's home page contains a link to information on how to report suspected fraud, waste, and abuse. The information has a link to the State Auditor's fraud reporting website and its hotline number, as well as information on the various ways to report suspected fraud internally. Institutional policies and procedures address the requirement to report fraud and the Standards of Conduct Guide, applicable to all employees, addresses the reporting of fraud. The intranet sites of the departments of Institutional Compliance and Auditing & Advisory Services contain information and links for reporting suspected fraud.