# The University of Texas Health Houston (UTHealth Houston)
# Internal Audit Annual Report for 2026

**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


**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 ..... 2**

**II. Internal Audit Plan for Fiscal Year 2026**
**Compliance with Texas Education Code, Section 51.9337(h) ..... 2**

**III. Consulting Services and Other Activities ..... 4**

**IV. External Audit Services ..... 5**

**V. External Quality Assurance Review (Peer Review) ..... 6**

**VI. Internal Audit Plan for Fiscal Year 2027**
**Compliance with Texas General Appropriations Act, Benefits Proportionality Audit Requirement ..... 7**

**VII. Reporting Suspected Fraud and Abuse ..... 11**

**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 2026

| Audit Number | FY 2026 Audit Plan Audit / Project | Description | Status | Report Date |
|---|---|---|---|---|
| ***Assurance Engagements*** | | | | |
| HSC26ASCF1461 | AI Governance (carried forward) | Review the controls over the use of externally available AI. | Complete | 06/09/2026 |
| HSC26ASCF1460 | Cancer Genomics Center (carried forward) | Review the efficiency and effectiveness of the Cancer Genomics Center. | Complete | 04/15/2026 |
| HSC26ASCF1466 | CIM-UTP (carried forward) | Review the operational and financial controls of UT Physicians. | Complete | 02/17/2026 |
| HSC26ASCF1464 | Inbound Email Security (carried forward) | Review controls around the inbound email security solution (Abnormal). | Complete | 10/31/2025 |
| HSC26ASCF1462 | UCT Data Center (carried forward) | Review controls over the UCT data center. *Also meets the biennial compliance requirement with the Texas Administrative Code Section 202.* | Complete | 09/08/2025 |
| HSC26AS1061 | Digital Accessibility | Review controls/compliance with digital accessibility standards. | Complete | 06/01/2026 |
| HSC26AS1045 | DSRDP | Review compliance with | Complete | 10/19/2026 |

| | | | | |
|---|---|---|---|---|
| | | DSRDP processes/bylaws based on assessed risk. | | |
| HSC26AS1053 | Epic Interfaces | Review controls around interfaces to/from Epic. | Complete | 09/01/2026 |
| HSC26AS1047 | Hard Drive Decommissioning | Review controls around hard drive decommissioning. | Complete | 08/31/2026 |
| HSC26AS1051 | Isilon System | Review controls around unstructured data storage (Isilon Storage System). Serves as TAC 202 engagement. | Complete | 10/20/206 |
| HSC26AS1044 | MSRDP | Review compliance with MSRDP processes/bylaws based on assessed risk. | Cancelled | |
| HSC26AS1049 | Physician Revenue | Review controls around physician revenue. | In Progress | |
| HSC26AS1568 | Review & Validation | Review controls around review & validation requirements per UTS 142 Financial Accounting and Reporting. | Complete | 10/31/2025 |
| HSC26AS1050 | System Owner Responsibilities | Review controls around the system owner program employed by IT Security. | Complete | 06/09/2026 |
| ***Required Engagements*** | | | | |
| HSC26RQ0932 | Epic Security Certification | Verify IT Security's control certification to Epic (annual requirement). | Complete | 02/16/2026 |
| HSC26RQ0931 | External Auditor Assistance | Assist the State Auditor's Office and other external audit functions. | Complete | No report Issued |
| HSC26RQ0929 | FY25 Financial Statements | Review controls over transactions and perform analytical reviews/other procedures assigned as part of the procedures for the FY25 financial statements. | Complete | Report issued by Deloitte at UT System level. |
| HSC26RQ0930 | FY26 Financial Statements | Perform interim procedures for the FY26 financial | Complete | Report issued by Deloitte at |

| | | | | |
|---|---|---|---|---|
| | | statements. | | UT System level. |
| ***Follow-Up*** | | | | |
| HSC26FL0813 | Follow-Up | Hours designated to perform periodic follow-up to validate the status of implementing outstanding recommendations | Complete | 9/1/2026 |

### 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 2026, 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 |
|---|---|---|---|
| HSC26ADCF1465 | Epic Payer Platform Advisory (carried forward) | Review whether security access controls around Epic Payer Platform are adequate and functioning as intended. | Results communicated to the department. |
| HSC26ADCF1463 | IT Security Vendor Risk Assessment Advisory (carried forward) | Review whether controls for third party vendor risk assessments are adequate and functioning as intended. | Results communicated to the department. |
| HSC26AD0821 | Data Analytics | Assisting departments with data analytic needs. | Results communicated to the department. |
| HSC26AD0037 | Expenditures Review Advisory | Annual testing of non-payroll expenditures. | Cancelled |
| HSC26AD0579 | Institutional Compliance Advisory | Review of UTHealth Houston's compliance program. | On FY27 Audit Plan as a carryforward. |

| | | | |
|---|---|---|---|
| HSC26AD0021 | Prohibited Technology Blocking Advisory | Review whether processes are in place to ensure compliance with the list of prohibited technologies/covered applications as published by the Texas Department of Information Resources and Texas Cyber Command. | Results communicated to the department. |
| HSC26AD1048 | Restricted Patient Records Advisory | An analysis of the false positives generated by Epic Break the Glass (BTG). | Results communicated to the department. |
| HSC26AD1057 | TEC 51.3525 | Assist management in ensuring compliance TEC 51.3525. | Results communicated to the department. |
| HSC26AD0714 | UTP Reconciliations Advisory | Review whether controls around UTP reconciliations are adequate and functioning as intended. | On FY27 Audit Plan as a carryforward. |

## IV. External Audit Services

| Service | Provider |
|---|---|
| Audit of Diversity, Equity, and Inclusion Requirements at Institutions of Higher Education | Texas State Auditor's Office |
| 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 2025 Assurance Work | Deloitte and Touche LLP (Deloitte) Certified Public Accountants |
| Financial Statements FY 2026 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 2025 and 2026 | Forvis Mazars, LLP Certified Public Accountants |

## V. External Quality Assurance Review (Peer Review)

bakertilly

October 2026

Dan Sherman, Vice President and Chief Audit Officer (CAO)
University of Texas Health Science Center at Houston (UTHealth Houston)

Internal audit (IA) functions perform their activities in accordance with the Global Internal Audit Standards (GIAS or the Standards) promulgated by the Institute of Internal Auditors (IIA), which were updated and went into effect in January 2025. UTHealth Houston's IA function, Auditing & Advisory Services, is also subject to Generally Accepted Government Auditing Standards (GAGAS) and the Texas Internal Auditing Act (TIAA). As required by these standards, UTHealth Houston's IA function completed its triennial external quality assessment by performing a self-assessment in June 2026, and engaged an independent review team to perform independent validation of that assessment. The primary objective of the validation was to verify whether the conclusions made in the quality self-assessment report regarding conformance with the GIAS, GAGAS, and the relevant requirements of the TIAA were adequately supported and reflected due professional care in the performance of the assessment.

In acting as an Independent Assessor, we attest to being fully independent of the organization and have the necessary knowledge and skills to undertake this engagement. The independent validation primarily consisted of interviews with key stakeholders and a review of the procedures and results of the self-assessment performed by UTHealth Houston Self-Assessment Team.

The IIA's *Quality Assessment Manual* suggests a scale of four ratings:

| Quality Rating | Conclusion Definition |
|---|---|
| **Fully Achieves** | "Full achievement" is the top rating and means that an IA function is fully achieving all 15 principles and the Purpose of Internal Auditing. |
| **Generally Achieves** | "General Achievement" means that an IA function is not fully achieving at least one principle but is achieving the Purpose of Internal Auditing. |
| **Partially Achieves** | "Partial Achievement" means the IA function is not fully achieving at least one principle, and the impact is significant enough to rate the function's overall achievement as partially achieving. |
| **Nonachievement** | "Nonachievement" means the IA function is not fully achieving at least one principle, and the impact is significant enough to rate the function's overall conclusion as nonachievement. |

Based on our independent validation of the EQA performed by UTHealth Houston's IA team, we concur with IA's overall conclusion that the IA function **Fully Achieves** the Standards, Principles, and Purpose of Internal Auditing in its report, as well as IA's conclusions regarding GAGAS and TIAA requirements. Our review also noted strengths as well as opportunities for enhancing the IA function.

This information has been prepared pursuant to a client relationship exclusively with, and solely for the use and benefit of, 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 UTHealth Houston.

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

Very truly yours,

Baker Tilly Advisory Group, LP

Baker Tilly Advisory Group, LP

## VI. Internal Audit Plan for Fiscal Year 2027

| FY 2027 Audit Plan<br>Audit / Project | Budgeted Hours | Description |
|---|---|---|
| ***Assurance Engagements*** | | |
| Admissions | 450 | Determine whether controls around admissions at the McGovern Medical School are adequate and functioning as intended. |
| Bellaire Station | 500 | Determine whether controls implemented at Bellaire Station are adequate and functioning as intended. |
| Clinical AI Usage | 450 | Determine whether controls around clinical AI usage are adequate and functioning as intended. |
| Enterprise Data Storage & Backup | 550 | Determine whether controls around enterprise data storage & backup are adequate and functioning as intended. |
| Hospital Partner Data | 500 | Determine whether controls around hospital partner data stored at UTHealth are adequate and functioning as intended. |
| DSRDP | 400 | Review compliance with DSRDP processes/bylaws based on assessed risk. |
| MSRDP | 400 | Review compliance with MSRDP processes/bylaws based on assessed risk. |
| Carry Forward | 800 | Carryforward of prior year engagements. |
| **Assurance Engagements Subtotal** | **4,050** | |
| ***Required Engagements*** | | |
| Epic Security Certification | 400 | Verify IT Security's control certification to Epic (annual requirement). |
| External Auditor Assistance | 200 | Assist the State Auditor's Office and other external audit functions. |
| FY26 Financial Statements | 90 | Review controls over transactions and perform analytical reviews/other procedures assigned as part of the procedures for the FY26 financial statements. |
| FY27 Financial Statements | 60 | Perform interim procedures for the FY27 financial statements. |
| Willed Body Program (WBP) | 400 | Determine whether UTHealth's WBP has adequate controls in place to ensure the receiving, storing, using, and transporting of cadavers or anatomical specimens and the disposing of remains comply with state law. |
| **Required Engagements Subtotal** | **1,150** | |

| | | |
|---|---|---|
| ***Advisory Engagements*** | | |
| Data Analytics | 300 | Assist management using data analytics. |
| Financial Advisory | 1,200 | Assist management in reviewing financial controls. |
| IT Advisory | 900 | Assist management in reviewing information technology controls. |
| Management Assistance | 100 | Assist management with requests. |
| UTHH Committees | 300 | Attend UTHH committees to monitor business developments. |
| **Advisory Engagements Subtotal** | **2,800** | |
| ***Reserve*** | | |
| Assurance/Advisory Reserve | 900 | Perform assurance/advisory engagements requested by management. |
| **Reserve Subtotal** | **900** | |
| ***Investigations*** | | |
| Investigations | 300 | Review possible cases of diversion 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*** | | |
| eCase/IDEA | 300 | Train, develop, and perform maintenance associated with eCase/IDEA. |
| 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. |
| FY 2028 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. |
| Internal Audit Committee | 500 | Prepare Internal Audit Committee packages and related post-meeting documentation. |

| | | |
|---|---|---|
| Internal Process Improvement | 350 | Review/update of A&AS audit processes. |
| 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. |
| Staff Meetings | 500 | Participate in regularly scheduled departmental staff meetings, manager meetings, and staff-only meetings. |
| **Operations Subtotal** | **2,400** | |
| ***Initiatives and Education*** | | |
| CPE/Training | 400 | Professional training and CPE courses to keep certifications active. |
| Professional Activities | 43 | Writing, publication, external presentations, and participation in professional organizations. |
| UT System Initiatives | 200 | Participation in UT System initiatives including committees, workgroups, etc. |
| **Initiatives and Education** | **643** | |
| **Total Budgeted Hours** | **12,843** | |

| High Risks Not Included in FY 2027 Audit Plan | Explanation / Mitigation | Internal Audit Action |
|---|---|---|
| Restructuring and transition of UTP administrative functions resulting in in operational inefficiencies and/or degradation of controls. | Audit coverage in prior two fiscal years | Report Submitted |
| Staff turnover has negative effect on patient experience, retention, revenue, or adequate oversight of funding. | Executive management support/review | Monitor Developments |
| TIPPS reporting methodology presents ongoing issues and uncertainty resulting in future lost funding and/or contract violations. | Executive management support/review | Monitor Developments |
| Heavy dependence on partners (e.g., Memorial Hermann, Harris Health, state of Texas) for funding resulting in financial uncertainty. | Executive management support/review | Monitor Developments |
| Inability to recruit candidates to fill open healthcare positions resulting in lost revenue and operational inefficiencies. | Executive management support/review | Monitor Developments |
| Noncompliance with NSPM 33 Research Security Program resulting in fines and other penalties. | Risk management function activity | Monitor Developments |
| Phishing attacks are successful resulting in a breach. | Executive management support/review | Monitor Developments |
| User shares credentials with agentic AI resulting in a breach, unintended actions, and/or inability to discern user activity logs. | Risk management function activity | Monitor Developments |

| | | |
|---|---|---|
| Successful social engineering against UTHealth executives resulting in a breach. | Risk management function activity | Monitor Developments |
| Delays in physician credentialing resulting in billing delays and financial losses. | Executive management support/review | Monitor Developments |
| Foreign entity influences on UTHealth operations resulting in noncompliance and reputational damage | Executive management support/review | 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-60, the General Appropriations Act (89th Texas Legislature) requires the following:

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 2027 annual risk assessment. It was not assessed as a high risk and therefore not included in the FY 2027 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.