
UT HEALTH SAN ANTONIO AUDIT COMMITTEE Q3 FY 2024

June 26, 2024



FY 2025 RISK ASSESSMENT
AND AUDIT PLAN



FY2025 RISK ASSESSMENT & AUDIT PLAN

Risk Assessment Methodology

Alignment – Risk Assessment &
Audit Plan

Changes in Risk Landscape

Focus on UT Health San Antonio

FY 2025 Internal Audit Plan
(Proposed)



RISK ASSESSMENT METHODOLOGY

Audit Plan designed to align with UT Health San Antonio's strategic objectives and core values

Assessed financial, operational, and compliance related risks

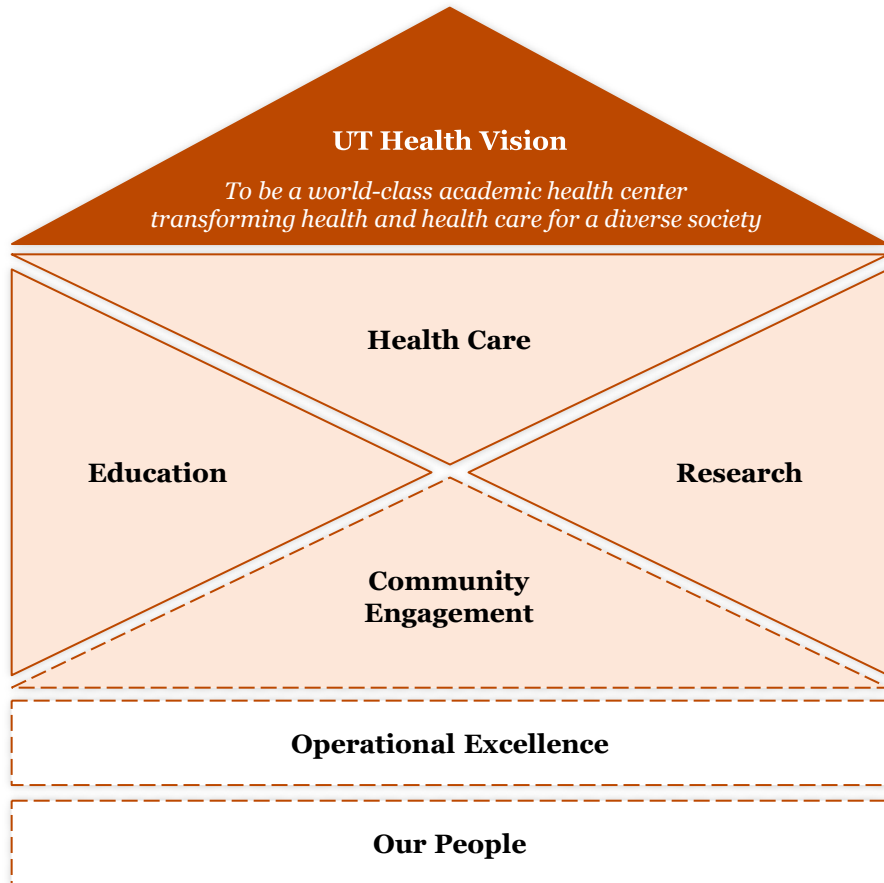
Risk Assessment focused on patient safety/care quality, regulatory compliance, financial risks, operational efficiency, research activities, crisis management/preparedness, data privacy and security

Solicited input from:

- Institutional leadership and key stakeholders
- Other Academic Medical Centers and Healthcare organizations including within the UT System
- Subject Matter Experts from prominent audit and consulting firms



ALIGNMENT – RISK ASSESSMENT & AUDIT PLAN



Key Initiatives/Activities Impacting Our Risk Landscape

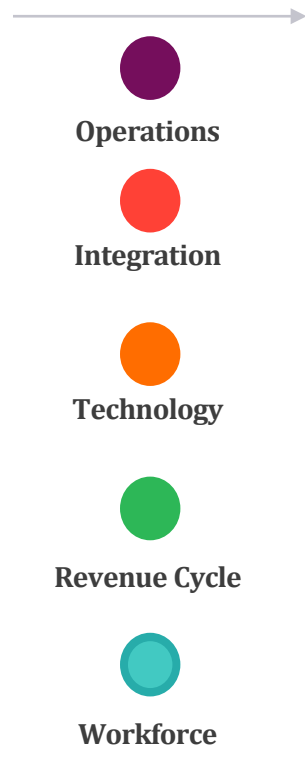
- Expansion of Health Care – Hospital (*scheduled to open late 2024*)
- New partnerships/business relationships
- Practice Plan – significant growth of clinical operations
- Significant growth in Research
- Expansion of Academic programs, including School of Public Health
- \$1B in capital/construction activities
- Financial management

Key Risk Themes

- Strategic
- Financial management
- Regulatory Compliance
- Clinical quality and patient safety
- Cybersecurity & Data Privacy
- Research integrity & funding
- Talent acquisition & Retention
- Business Continuity & Resiliency

CHANGES IN THE MARKET

Emerging Risks



Changes in the Market

- Economy
- Adapting to changing consumer needs, demands, and expectations
- Creating financial sustainability with value-based care
- New care delivery models
- Investing in digital innovation and transformation
- New and increasing regulatory requirements (Federal & State)
- Changes in reimbursement model and cost containment
- Talent acquisition, retention, development, depth, burnout
- Robotic Process Automation and Artificial Intelligence, Big Data

Effective Risk Management

- Enables strategic initiatives Decreases the risk profile of the institution
- Delivers innovation, coordination and efficiency in the institution's approach to risk
- Enables organizational strategy and operational success
- Enhances the control environment
- Drives business insights
- Decreases the risk profile

Upside Risks

Risks that offer benefits. Risks significant to an organization's ability to achieve its strategic objectives.

- Innovations
- Increasing market reach
- Acquiring, managing, and deriving value from new assets and talent

Outside Risks

Risks that offer negative or positive benefits beyond the organization's control

- Actions of existing and emerging competitors
- Geopolitical and economic trends
- Demographic and environmental trends

Downside Risks

Risks that offer negative impacts. Risks an organization is focused on eliminating, avoiding, mitigating or transferring in a cost-effective manner.

- Information security and cybercrime
- Employee fraud, and regulatory compliance
- Risks must be well understood and mitigated

FOCUS ON UT HEALTH SAN ANTONIO'S ENVIRONMENT

Education | Research | Health Care | Community Engagement

UT Health SA Experience	System Sustainability	Regulatory Compliance	Data Excellence and Protection
<ul style="list-style-type: none">• Patient access, clinical and financial experience• Employee excellence• Provider/Physician Enterprise• Students• Payor strategy• Business partners• Communities	<ul style="list-style-type: none">• Revenue cycle• Margin management• Operational Continuity• Supply chain and third-party risk management• Facilities and environment• Ability to hire and sustain qualified staff	<ul style="list-style-type: none">• State of Texas• CMS and Federal• Privacy & Data Security• Governance, training, reporting and COI• Telemedicine• Integrated compliance execution• Monitoring• Stark Law (Physician Referrals)• FERPA (Family Educational Rights & Privacy Act)	<ul style="list-style-type: none">• Data analytics and decision making• Reporting and data governance• EHR and ERP optimization• Remote Workforce• Cybersecurity• Robotic Process Automation• Artificial Intelligence

FY 2025 AUDIT PLAN *

Governance	Revenue Cycle	Clinical Operations	Cyber Security & Data Privacy	Regulatory/ Compliance	Legend
<ul style="list-style-type: none"> Supply Chain Management – (non-contracted) Vendor Usage Physical Security & Environmental Protection of IT Assets (SoPH) 	<ul style="list-style-type: none"> Controllable Write-Offs Revenue Cycle – Central Verification 	<ul style="list-style-type: none"> Physician Credentialing axiUm – Epic (Wisdom) Pre-Implementation Epic Hosting Information Security Medical Device Management Epic System – UHS Business/Operations Continuity Plan – Clinical Practice Hospital Advisory Services (IT & Operations) 	<ul style="list-style-type: none"> Access Management & Identity Governance (TAC 202) Decentralized IT Operations and Security Governance Patch Management Peoplesoft -Oracle HCM Implementation (Wave 2) Privileged Access Management – Netwrix Web and API Security IT Asset Management Governance over AI 	<ul style="list-style-type: none"> Sub-certification Process and Monitoring of Key Controls Records Release Process – HIPAA Compliance Controlled Substances – Research NIH Grant Review – Expenditures State Contracting F/U SB17 Compliance Residency Program Award / Family & Community Medicine Annual Internal Audit Report (SAO) / Procurement Policies Assessment 	<ul style="list-style-type: none"> Risk-Based Audit Consulting Engagement Regulatory / Required Audit Below The Line Audit/Project (Work that will not be performed due to prioritization/lack of resources)
<ul style="list-style-type: none"> Foreign Influence 	<ul style="list-style-type: none"> Payor Contract Compliance Mays Cancer Center Infusion Charge Capture and Billing Revenue Cycle – SoD Claims Processing Telemedicine 	<ul style="list-style-type: none"> Inventory Management – SoD Physical Security & Environmental Protection (Hospital) 	<ul style="list-style-type: none"> Risk Mgmt., Information Security & Compliance (RISC) Services Use of Prohibited Technologies 	<ul style="list-style-type: none"> Travel & Entertainment TX-RAMP (TGC 2054.0593) 	

* See Appendix A - Includes FY 2025 Audit Plan with a brief description of the audit/project

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

Risk-Based Audits	Preliminary Objective
Record Release Process - HIPAA	Determine if adequate controls are in place to ensure patient data is released timely and within federal, state, and Institutional policy.
Controlled Substances - Research	Assess the process and procedures in place to ensure compliance with pertinent federal, state, and Institutional requirements.
Controllable Write-Offs - UTHP	Evaluate the efficiency and effectiveness over billing and collections as it pertains to controllable write-offs for UTHP.
Revenue Cycle - Central Verification	Determine whether the central verification process is operating effectively and efficiently in obtaining proper authorizations needed to collect on filed claims.
NIH Grant Review - Expenditures	Assess the process and procedures regarding NIH grant expenditures to determine compliance with pertinent requirements.
Physician Credentialing	Assess MSRDP processes for: physician credentialing, recredentialing and monitoring of physician's licensures and insurance for expirations to ensure compliance with government regulations and Institutional policy.
Monitoring of Key Financial Controls - UTS 142	Validate the Institutional monitoring plan related to segregation of duties and account reconciliations and financial review and analysis.

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

Risk-Based IT Audits	Preliminary Objective
Access Management & Identity Governance (TAC 202)	Ensure that the right individuals have the appropriate access to technology resources while preventing unauthorized access that could lead to security breaches, data loss, and regulatory non-compliance.
Decentralized IT Operations and Security Governance	Establish and enforce security policies, controls, and procedures to protect IT assets and data and ensure decentralized IT operations comply with relevant regulations, standards, and policies.
axiUm - Epic (Wisdom) Pre-Implementation	Ensure the new system performs efficiently, delivers reliable results, and meets performance expectations. The assessment areas to cover are Data Conversion, Application Interface, IT Processes, Segregation of Duties, and Reporting, Hypercare/Warranty phase, to mention a few.
Epic Hosting Information Security	Ensure the security, integrity, confidentiality, and availability of information resources.
Medical Device Management - Hospital	Ensure the effective management, maintenance, and security of medical devices to provide safe and reliable healthcare services.
Patch Management	Ensure that software updates and patches are applied promptly and effectively to protect systems from vulnerabilities and maintain operational integrity.

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

Risk-Based IT Audits	Preliminary Objective
Peoplesoft - Oracle HCM Implementation - Wave 2	Ensure the new system performs efficiently, delivers reliable results, and meets performance expectations. The assessment areas to cover are Data Conversion, Application Interface, IT Processes, Segregation of Duties, and Reporting, Hypercare/Warranty phase, to mention a few.
Privileged Access Management - Netwrix	Securing and managing the elevated access rights of privileged accounts to prevent unauthorized access, data breaches, and insider threats.
Epic System- University Health System	Ensure the successful implementation and operation of the Epic electronic health record (EHR) system within a community healthcare setting.
Web and API Security	Ensure the protection of web applications and APIs from various threats and vulnerabilities to maintain data and services' confidentiality, integrity, and availability.

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

Consulting Engagements	Preliminary Objective
Supply Chain Management - (non-contracted) Vendor Usage	Assess the usage of non-contractual vendors to determine possible cost savings.
Physical Security & Environmental Protection of IT Assets (School of Public Health)	Ensure the safety and security of physical assets, including personnel, hardware, and facilities, from physical threats and environmental hazards.
State Contracting Follow-up	Assess management's action plans regarding recommendations from external reviews.
SB17 Compliance	Assess management's monitoring program for compliance to SB 17 (TEC 51.3525).
Hospital Advisory Services - Operations	Dedicated reserve hours for operational consulting and advisory services to support the opening of the new Research Hospital in December 2024, ensuring that performance expectations are met.

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

Consulting Engagements - IT	Preliminary Objective
Business/Operational Continuity Plan - Clinical Practice	Ensure an organization’s resilience during crises and minimize disruptions.
IT Assets Management	Ensure effective management of the lifecycle of the institution's IT assets to maximize value, control costs, and mitigate risks.
Governance over Artificial Intelligence	Protecting sensitive data and mitigating IT risks within an organization.
Hospital Advisory Services - IT Systems	Reserved hours for IT consulting/advisory services for new Research Hospital due to open Dec 2024.

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

Regulatory/Required Audits	Preliminary Objective
FY 2024 Financial Statement Audit Assistance (Year-end)	Assist the external auditors in the coordination and/or performance of testing for the audit of the Annual Financial Report (FY 24 year-end work).
FY 2025 Financial Statement Audit Assistance (Interim)	Assist the external auditors in the coordination and/or performance of financial and IT control testing for the audit of the Annual Financial Report (FY 25 interim work).
Residency Program Award/Family & Community Medicine	Review expenditures for the Residency program and report on the compliance with grant regulations to the Texas Higher Education Coordinating Board.
SAO Annual Reporting Requirement on Procurement Policies	Review for compliance with the Texas Education Code §51.9337 requirement that the chief audit executive annually certify to the state auditor that the institution has procurement policies in place that comply with the Texas Education Code requirements for higher education institutions.

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

“Below the Line” Audits/Projects *	Preliminary Objectives
Revenue Cycle - SoD Claims Processing (Consulting)	Assess the efficiency and effectiveness of the SoD billing and claims process and procedures.
Inventory Management - SoD (Consulting)	Assess the efficiency and effectiveness of the SoD inventory management process and procedures.
Payor (Insurance Carrier) Contract Compliance (Revenue)	Evaluate the effectiveness of payment collection processes and controls for payments received by insurance payors to ensure that UTHP is paid the agreed upon rates from payor contract(s).
Telemedicine	Assess the adequacy and effectiveness of the processes and controls for telemedicine services.
Mays Cancer Center Infusion Charge Capture and Billing	Assess the adequacy and effectiveness of the Mays Cancer Center's drug infusion charge capture and billing processes and controls.

“Below the Line” Audits/Projects will not be included in the FY 2025 Audit Plan due to prioritization/lack of resources

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

“Below the Line” Audits/Projects *	Preliminary Objectives
Physical Security & Environmental Protection - Hospital	Ensure the safety and security of physical assets, including personnel, hardware, and facilities, from physical threats and environmental hazards.
Foreign Influence	Evaluate the system of internal controls in place to manage risks identified by the federal government related to foreign influence.
Travel & Entertainment	Evaluate and test compliance with UT Health San Antonio and UTS policies for travel and entertainment expenses. (Required by UT System biennially - being done off-cycle based on risk).

“Below the Line” Audits/Projects will not be included in the FY 2025 Audit Plan due to prioritization/lack of resources

APPENDIX A – FY 2025 INTERNAL AUDIT PLAN

“Below the Line” IT Audits/Projects *	Preliminary Objectives
Risk Management, Information Security, and Compliance (RISC) Services	Ensure that the organization's risk management, information security, and compliance frameworks are robust and effective in protecting assets, maintaining regulatory compliance, and managing risks.
TX-RAMP: Texas Risk & Authorization Management Program (TGC 2054.0593)	Ensure that cloud computing services used by state agencies meet the necessary security and compliance requirements to protect sensitive information and maintain operational integrity.
Use of Prohibited Technologies	Ensure that the organization adheres to policies and regulations that forbid the use of certain technologies, tools, or software to mitigate various risks.

“Below the Line” Audits/Projects will not be included in the FY 2025 Audit Plan due to prioritization/lack of resources

APPENDIX B – FY 2025 INTERNAL AUDIT PLAN/BUDGET

<i>FY 2025 Audit Plan</i>	
<i>Project Name</i>	<i>Budget</i>
<i>Assurance Engagements</i>	<i>6,280</i>
<i>Advisory Engagements</i>	<i>3,560</i>
<i>Required Engagements</i>	<i>360</i>
<i>Investigations</i>	<i>380</i>
<i>Reserve</i>	<i>400</i>
<i>Follow-Up</i>	<i>320</i>
<i>Development - Operations</i>	<i>2,188</i>
<i>Development - Initiatives and Education</i>	<i>1,868</i>
<i>Total Budgeted Hours</i>	<i>15,356</i>