UT San Antonio FY27 Audit Plan

Campus	Engagement Title	Budget	Risk	Engagement Objectives
Assurance Engagements				
both	Research Data Access Controls Assessment-Aligned with NSPM-33 Security Requirements	450	Critical	The objective of this audit is to evaluate whether the institution has established and implemented effective governance, policies, and technical controls to manage and restrict access to sensitive research data in accordance with National Security Presidential Memorandum-33 (NSPM-33) research security requirements.
both	Operating Systems and Database Security Controls Review	400	Critical	To evaluate whether the institution has established and implemented effective security controls over operating systems and database environments to protect institutional systems and sensitive data. The review will assess whether operating systems and databases are securely configured in accordance with established standards, including hardening guidelines and patch management practices, and whether vulnerabilities are identified and remediated in a timely manner. Additionally, the audit will evaluate controls over user and privileged access to database systems, encryption of sensitive data, and logging and monitoring of system and database activities. The audit will also assess whether governance and oversight processes are in place to ensure consistent implementation of security controls across decentralized environments and to support compliance with regulatory and institutional security requirements.
both	Data Sharing & Data Use Governance Review	300	Critical	Assess governance over data sharing agreements, including approvals, data use limitations, and monitoring of data exchanges with third parties, research collaborators, and affiliates.
health	Drug Diversion	400	Critical	To evaluate the effectiveness of controls in preventing, detecting, and mitigating drug diversion, ensuring compliance with regulations and safeguarding the integrity of controlled substance management.
health	Medication Management	400	Critical	Determine the adequacy of controls to ensure safe medication practices for high-alert and look-alike/sound-alike (LASA) medications, including sample medications, related to labeling, storage, dispensing, and administration in Hospital Outpatient Department (HOPD) clinics in compliance with Joint Commission requirements.
health	Physician Credentialing	400	Critical	Assess the effectiveness of MSRDP credentialing and recredentialing processes for physicians practicing within the clinical practice plan and hospital, including ongoing monitoring of licensure and insurance expirations, to ensure compliance with applicable government regulations and Institutional policies.
health	Informed Consent - Clinical Operations / MSRH	450	Critical	To determine whether the organization's informed consent processes are compliant with regulatory and accreditation requirements and ensure that patients (or authorized representatives) provide informed, documented, and timely consent prior to treatment or procedures.
health	Sterilization and High-level Disinfection - Instruments	450	Critical	To determine whether the sterilization and high-level disinfection processes for reusable medical devices and instruments are designed and operating effectively to ensure patient safety, regulatory compliance, and reliable clinical operations across hospital and clinical practice settings.
health	Supply Chain Management - Hospital	450	Critical	Assess whether the hospital has established and is effectively implementing supply chain management processes and controls to ensure continuous availability of critical supplies necessary for safe and effective patient care and compliance with regulatory requirements.

UT San Antonio FY27 Audit Plan

Campus	Engagement Title	Budget	Risk	Engagement Objectives
health	Procurement - Payment Request Usage	500	Critical	Assess whether payment requests are used in accordance with institutional procurement policies and State of Texas requirements, and to determine whether excessive reliance on payment requests in lieu of purchase orders undermines key purchasing controls, competitive procurement requirements, fiscal oversight, and compliance with applicable laws, regulations, and funding restrictions.
health	Hospital - Staff Competency	400	Critical	Assess whether the hospital has designed and implemented effective processes to ensure staff competency is defined, documented, monitored, and validated in compliance with Joint Commission, CMS, and other regulatory requirements, in the absence of an integrated electronic competency management platform.
health	Critical Lab Values & Care Coordination	400	Critical	Assess whether processes, controls, and accountability structures for managing critical lab values are effectively designed, implemented, and consistently followed across care settings to ensure timely identification, communication, and resolution of critical results, thereby reducing patient safety risks and liability exposure.
health	Foreign Influence - Controls over Visiting Scholars and Foreign Researchers	300	Critical	Determine whether processes and controls are in place for visiting scholars and foreign researchers to include appropriate vetting, approval, access controls, and ongoing monitoring.
health	EPIC Hosting Information Security	350	Critical	To evaluate whether the organization has established and implemented effective governance, policies, and technical controls to secure systems, endpoints, infrastructure, and user access associated with Epic-hosted environments in accordance with organizational security responsibilities, industry cybersecurity practices, and Epic contractual requirements.
health	Research - (Controlled Substances) - Carry Forward	100	Critical	Carryover project from FY26 Audit Plan. Assess the process and procedures in place to ensure compliance with pertinent federal, state, and Institutional policy.
academic	Athletics IAM & Access Governance Audit	300	Critical	The objective of this audit is to evaluate whether the Athletics Department has established and implemented effective identity and access management (IAM) governance and access control processes over systems, applications (Teamworks), and data supporting athletics operations. The review will assess whether user access to athletics-related systems, including recruiting platforms, ticketing systems, donor and booster applications, student-athlete information systems, financial systems, collaboration tools, and third-party cloud applications, is appropriately authorized, provisioned, modified, and revoked in a timely manner based on job responsibilities and least-privilege principles. The audit will also evaluate the effectiveness of authentication controls, privileged access management, segregation of duties, periodic access reviews, and monitoring of user activity. In addition, the review will assess governance over shared accounts, student worker access, coach and contractor access, and integration with centralized institutional identity management processes to ensure protection of sensitive student-athlete, financial, medical, and operational data.

UT San Antonio FY27 Audit Plan

Campus	Engagement Title	Budget	Risk	Engagement Objectives
academic	Third-Party Security Risk Management	300	Critical	The objective of this audit is to evaluate whether the institution has established and implemented effective governance, processes, and controls for identifying, assessing, and managing third-party security risks throughout the vendor lifecycle. The review will assess whether third-party vendors are appropriately risk-ranked based on the sensitivity of data accessed and services provided, and whether security due diligence; such as risk assessments, review of SOC reports, contractual security requirements, and compliance with applicable regulations; is performed prior to onboarding. Additionally, the audit will evaluate whether ongoing monitoring processes, including periodic risk reassessments, access reviews, and vendor performance oversight, are in place to ensure third-party risks are continuously identified, managed, and mitigated in alignment with institutional policies and regulatory expectations.
academic	Vulnerability & Patch Management	300	Critical	To evaluate whether the organization has established and is effectively operating a comprehensive vulnerability and patch management program to ensure that security vulnerabilities are timely identified, risk-ranked, remediated, and monitored across in-scope systems. This includes assessing governance and accountability, vulnerability scanning and assessment processes, patch testing and deployment practices, exception and remediation management, and monitoring and reporting mechanisms to determine whether vulnerabilities are addressed in alignment with defined risk tolerances, security standards, and regulatory or institutional requirements.
academic	Name, Image, and Likeness and Revenue Share Review	400	Critical	Assess the design and operating effectiveness of controls over NIL and revenue-sharing activities to ensure compliance with regulatory requirements, proper governance, accurate financial reporting, and mitigation of legal and reputational risk.
academic	Award Management Finance Lifecyle	350	Critical	Assess whether controls over the award management financial lifecycle ensure compliant, accurate, and timely financial management, reporting, and closeout of sponsored awards.
academic	Research Security and Foreign Influence Compliance Review	400	Critical	Evaluate whether the institution has established and is effectively implementing policies, procedures, and controls to ensure compliance with GA-48 and House Bill 127 requirements related to foreign influence, critical infrastructure protection, Research Security Council, etc.
academic	Physical Access Control Remediation Review	350	Critical	Ensure physical access is properly granted, timely removed, and restricted areas are well controlled by confirming prior audit findings have been remediated.
academic	TX-RAMP: Texas Risk & Authorization Management Program (TGC 2063.408)	250	High	To evaluate whether the institution has established effective governance, procurement controls, and monitoring processes to ensure compliance with the Texas Risk and Authorization Management Program (TX-RAMP) requirements under Texas Government Code (TGC) 2063.408.
academic	Athletics Operations	400	High	Strengthen operations by validating that gap assessment controls are implemented and operating effectively.
academic	Decentralized Gift Acceptance Governance and Compliance Review	375	High	Assess the effectiveness of governance structures and internal controls in ensuring gifts are consistently accepted and processed through required centralized procedures, promoting compliance, accurate reporting, and protection of the university's reputation.
academic	Americans with Disabilities Act Digital Accessibility Compliance	450	High	Determine whether the institution's governance, controls, and execution are sufficient to achieve and sustain compliance with ADA Title II digital (web and mobile) accessibility requirements.

UT San Antonio FY27 Audit Plan

Campus	Engagement Title	Budget	Risk	Engagement Objectives
academic	IT General Controls Assessment (Access & Change Management)- College of Business- TAC202	200	High	The objective of this audit is to evaluate whether the College of Business has established and implemented effective IT general controls over user access management and change management processes for critical business applications, databases, and supporting systems. The review will assess whether access to systems and sensitive data is appropriately authorized, provisioned, modified, and revoked in a timely manner based on job responsibilities and least-privilege principles. The audit will also evaluate the effectiveness of authentication controls, periodic access reviews, privileged access management, and segregation of duties. In addition, the audit will assess whether system changes, configuration updates, interfaces, and application modifications are formally documented, tested, approved, implemented, and monitored to minimize the risk of unauthorized changes, operational disruptions, data integrity issues, or security vulnerabilities within the Colleges decentralized IT environment.
academic	IT General Controls Assessment (Access & Change Management)- Procore - TAC202	200	High	The objective of this audit is to evaluate whether the academic construction team has established and implemented effective IT general controls over user access management and change management processes for critical business applications, databases, and supporting systems. The review will assess whether access to systems and sensitive data is appropriately authorized, provisioned, modified, and revoked in a timely manner based on job responsibilities and least-privilege principles. The audit will also evaluate the effectiveness of authentication controls, periodic access reviews, privileged access management, and segregation of duties. In addition, the audit will assess whether system changes, configuration updates, interfaces, and application modifications are formally documented, tested, approved, implemented, and monitored to minimize the risk of unauthorized changes, operational disruptions, data integrity issues, or security vulnerabilities within the Colleges decentralized IT environment.
both	Procurement and Contracting Practices (TEC §51.9337)	350	High	Review the procurement and contracting processes of goods/services within the UT San Antonio Contract Management Handbooks to ensure the controls in place are working as intended. (Satisfies the review for compliance with the Texas Education Code §51.9337 requirement to allow the chief audit executive to annually certify to the state auditor that the institution has procurement policies in place.) (Due 11/1/26)
both	Cybersecurity & AI Training (TGC 2054.5191 & 2063.104)	200	High	To evaluate whether the institution has established and implemented effective processes, controls, and monitoring mechanisms to ensure compliance with the cybersecurity and Artificial Intelligence (AI) training requirements mandated under Texas Government Code (TGC) 2054.5191 and 2063.104.
both	Use of Prohibited Technologies	250	High	To evaluate whether the institution has established and implemented effective policies, technical controls, and monitoring mechanisms to ensure compliance with the State of Texas prohibited technologies requirements.
both	Information Security Exception Governance Review	200	High	To evaluate whether the institution has established and implemented effective governance, processes, and controls for managing information security exceptions in alignment with institutional policies and regulatory requirements. The review will assess whether exceptions to security standards are formally documented, include appropriate risk assessments and compensating controls, and are reviewed and approved by authorized personnel. Additionally, the audit will evaluate whether exceptions are tracked, time-bound with defined expiration dates, periodically revalidated, and monitored to ensure continued relevance and risk mitigation. The audit will also assess whether oversight and reporting mechanisms are in place to provide transparency to management and ensure that exceptions are appropriately governed and do not introduce unacceptable levels of risk.
Budget for Assurance Engagements		**11,025**	**43.8%**	

UT San Antonio FY27 Audit Plan

Campus	Engagement Title	Budget	Risk	Engagement Objectives
Advisory Engagements				
both	FERPA Compliance and Third-Party Student Data Protection Review	350	Critical	The objective of this engagement is to evaluate whether the institution has established and implemented effective policies, procedures, contractual safeguards, and internal controls to protect student education records in accordance with FERPA requirements, with specific focus on third-party systems and vendors that access, store, transmit, or process student data, including Canvas and related learning technology integrations. The review will assess whether vendor contracts include appropriate data protection, confidentiality, access restriction, data use, breach notification, data retention, and disposal provisions, and whether institutional processes exist to monitor third-party compliance with FERPA and internal privacy requirements.
both	Enterprise Identity and Access Management Governance Review - TAC202	450	Critical	The objective of this engagement is to evaluate whether the institution has implemented effective enterprise IAM governance and controls across federation and authentication, Zero Trust security, access lifecycle management, privileged access, access recertification, monitoring, and oversight of identity-related risks across academic, clinical, research, and administrative systems.
both	Shadow AI & Data Protection	200	Critical	To assess risks related to unmanaged AI usage, including data input controls, user awareness, and monitoring of AI tools.
both	AI Data Privacy & PHI Protection Review	300	Critical	The objective of this review is to evaluate whether the institution has established and implemented effective governance, privacy controls, and monitoring processes over the use of artificial intelligence (AI) technologies that access, process, store, transmit, or generate sensitive institutional, clinical, research, employee, or patient data, including protected health information (PHI). The review will assess whether AI-related activities comply with HIPAA, privacy regulations, institutional data governance standards, and acceptable use requirements. The engagement will evaluate controls over data input restrictions, data classification, anonymization and de-identification practices, user awareness, access controls, logging and monitoring, retention of AI-generated outputs, and approval processes for AI-enabled tools. Additionally, the review will assess whether safeguards exist to prevent unauthorized disclosure of sensitive data through public or third-party AI platforms and whether monitoring and oversight processes adequately address emerging privacy and ethical risks associated with AI usage across clinical, academic, research, and administrative functions.
both	AI Vendor Risk Assessment	300	Critical	The objective of this assessment is to evaluate whether the institution has established effective governance, due diligence, procurement, and ongoing monitoring processes over third-party artificial intelligence (AI) vendors, platforms, and service providers utilized across academic, clinical, research, and administrative operations. The review will assess whether AI vendors are appropriately evaluated for cybersecurity, privacy, regulatory compliance, data ownership, model transparency, ethical considerations, contractual protections, and operational resilience prior to implementation and throughout the vendor lifecycle. The assessment will also evaluate whether AI-related vendor agreements include appropriate provisions addressing data protection, PHI handling, model accountability, incident notification, audit rights, intellectual property, and compliance with institutional and regulatory requirements. Additionally, the review will assess governance over decentralized procurement and monitoring practices to determine whether unmanaged or high-risk AI vendor relationships introduce cybersecurity, operational, financial, legal, or reputational risks to the institution.

UT San Antonio FY27 Audit Plan

Campus	Engagement Title	Budget	Risk	Engagement Objectives
both	Integration - (UTSA/UT Health SA)	772	Critical	Dedicated reserve hours for operational consulting and advisory services to support integration efforts between the health and academic campuses.
health	Business Continuity Plan – EMR Downtime (Hospital/Clinical Operations)	250	Critical	Assess whether downtime and business continuity processes—including governance, standardized workflows, and operational readiness for clinical care—are effectively designed, implemented, and tested to ensure continuity of safe patient care during system outages or cyber events.
health	Health Campus Physical Security	350	Critical	Assess whether physical security controls (including access management, surveillance, and monitoring) are adequately designed and operating effectively to safeguard people, facilities, and assets across campus, ambulatory clinics, and hospital settings.
health	Accessibility - Healthcare	320	Critical	To determine whether UT San Antonio health campus has established and implemented effective governance, policies, controls, and monitoring processes to ensure compliance with ADA Title II digital accessibility requirements (WCAG 2.1 Level AA) across academic, clinical, and hospital operations, including the new hospital, and whether digital services are accessible, consistently applied, and adequately monitored.
health	MSRDP - Advisory Services - Operations/Financials	340	Critical	Dedicated reserve hours for operational consulting and advisory services to support MSRDP HOPD clinical/hospital practices.
health	AI Enabled Mobile Applications	320	Critical	To assess whether the institution has established and implemented effective governance, clinical oversight, security, and compliance controls over the use of AI-enabled mobile applications for recording patient encounters, to ensure clinical documentation accuracy, protection of PHI, regulatory compliance, and appropriate physician accountability.
health	Be Well, Texas - Disbursements	450	Critical	Assess the process ad procedures regarding BWTX program expenditures to determine compliance with pertinent requirements.
health	SoD - Clinical Operations/Financial	120	Critical	Dedicated reserve hours for operational consulting and advisory services to support the School of Dentistry's (SoD) clinical practice.
academic	Student Mental Health Services	250	Critical	Evaluate the alignment of student mental health initiatives with institutional priorities and the organization and oversight supporting implementation.
academic	Financial Aid Quality Control (QC) Program	350	Critical	Assess and advise on strengthening Financial Aid Quality Control processes to improve risk detection, remediation, and compliance with Title IV.
academic	Student Lifecycle Fraud Risks	150	High	Evaluate and provide insight on a coordinated framework for identifying and sharing student fraud risks (ghost students) to enable early detection and reduce institutional risk.
academic	IT Governance & Decentralization Oversight	250	High	To evaluate governance structures, policies, and oversight mechanisms across decentralized IT environments.
academic	Data Center Infrastructure - Carry Forward	200	High	To evaluate the adequacy, efficiency, and resiliency of the data center infrastructure supporting institutional operations, with specific focus on capacity management, redundancy, environmental controls, and alignment with current and future organizational growth.

UT San Antonio FY27 Audit Plan

Campus	Engagement Title	Budget	Risk	Engagement Objectives
both	Institutional Strategic Initiatives/Communication with Stakeholders	320	Medium	Participate in Institutional initiatives focused on adding value and enhancing quality. Attend campus committees and other meetings with management.
both	Meetings with Institutional Leadership	370	NA	Regularly scheduled, and as needed, meetings with the top 50+ leaders across the Institution to ensure that IA is aware of current and upcoming key initiatives and projects across the Institution. These meetings serve as a key element in: continually assessing the risk landscape, ensuring that Audit resources are focused on areas most critical to the Institution and that we have a consistent view of the strategic objectives of UT Health SA. These meetings also help to identify opportunities for IA to provide consulting services.
	Budget for Advisory Engagements	**6,412**	**25.5%**	
Required Engagements				
academic	FY26 State Auditor's Office Single Audit	50	Critical	Assist and coordinate with the State Auditor's Office for the FY 2026 Statewide Single Audit of Student Financial Aid. (Due February 2027)
academic	NCAA Agreed Upon Procedures	25	High	Assist with the required NCAA Agreed Upon Procedures for FY 2026. The UT System Audit Office will use a 3rd-party service provider to perform the NCAA-agreed-upon procedures. (Due 1/15/27)
both	FY26 Financial Statement Audit	139	Medium	Review of UT San Antonio financial statements (academic and health campuses) in support of Deloitte's UT System Consolidated Financial Statement work for FY 2026.
both	FY27 Financial Statement Audit (Interim)	96	Medium	Perform interim testing for in support of Deloitte's UT System Consolidated Financial Statement work for FY 2027.
both	Audit Assistance to External Agencies (SAO, THECB, etc.)	20	Medium	Coordinate external agency audits.
	Budget for Required Engagements	**330**	**1.3%**	
	Investigations Budget	**550**	**2.2%**	
	Follow-Up Budget	**470**	**1.9%**	
	Reserve Budget	**200**	**0.8%**	
	Initiatives and Education Budget	**1,839**	**7.3%**	
	Operations Budget	**4,343**	**17.3%**	
	Total Budget	**25,169**	**100.0%**	