UTHealth Houston
Auditing and Advisory Services
P.O. Box 20036 | Houston, TX | 713-500-3160

Artificial Intelligence Governance

HSC25AS0001

EXECUTIVE SUMMARY

Auditing & Advisory Services (A&AS) has completed an assurance engagement of artificial intelligence (AI) governance. This engagement was performed at the request of the UTHealth Houston (UTHealth) Audit Committee and was conducted in accordance with the Global Internal Audit Standards.

Background

AI governance is the framework of policies, processes, and controls that guide the responsible development, deployment, and oversight of AI Systems. Effective AI governance ensures AI Systems are transparent, accountable, fair, and secure while encompassing strategic alignment, risk management, and regulatory compliance.

Objectives

Our objective was to determine whether governance around AI deployment is adequate. Specifically, to determine if:

- The AI Governance & Policy Subcommittee (Subcommittee) meets on an ongoing basis.
- The standard vendor contract prohibits vendors from using data for training AI models.
- AI usage and Heightened Scrutiny Artificial Intelligence System (HSAIS) criteria is reviewed and considered during software procurement.
- Vendor assessments of AI Systems are reasonable and complete.
- Impact assessments are completed, monitored, and documented for any HSAIS AI Systems.
- AI risk and impact questions are included in the standard vendor assessment used by Information Security.

Scope Period

AI System inventory as of February 28, 2026 and software purchases/AI assessments between January 1, 2026 and February 28, 2026

Conclusion

Overall, governance around AI deployment is adequate. We noted the following opportunities for improvement:

#	Observation Summary	Risk	Risk Rating
1	Software purchases are not consistently assessed to determine if they should be classified as HSAIS.	Lack of AI System oversight and potential regulatory noncompliance.	**High**
2	Policies have not been updated to reflect the current business process.	Noncompliance with policy.	**Medium**

OBSERVATIONS & MANAGEMENT RESPONSES

#1 – Risk Assessments

Cause
Software purchases are not consistently assessed to determine if they should be classified as Heightened Security Artificial Intelligence Systems (HSAIS).

Risk
Lack of AI System oversight and potential regulatory noncompliance.

Condition
We reviewed 15 software purchases (14 renewals and 1 new purchase) over $100K within the scope period. We noted six renewals and one new purchase were not assessed for HSAIS classification by Information Security.

Management informed us system owners are responsible for requesting risk assessments (which includes HSAIS classification) to be conducted by Information Security.

Criteria
Handbook of Operating Procedures (HOOP) 235 Governance and Use of Artificial Intelligence requires Information Security to conduct a review of each AI System submitted to the AI System inventory to determine HSAIS classification.

Recommendations
Procurement and Information Security should work together to develop and implement a process to ensure risk assessments (including HSAIS classification) are completed for all software purchases.

Rating
High

Management Response #1
A question will be added to Coupa for all software procurement requests to identify whether the software utilizes AI. This will trigger a notification to Information Security that an assessment will need to be completed.

Responsible Party
Eric Williams, Vice President Supply Chain Management
Job Finney, Director, Business Process Management & Analytics

Implementation Date
June 15, 2026

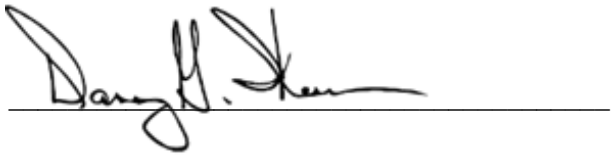
Management Response #2
Information Security is creating an HSAIS checklist based on the criteria defined in SB 1964 with guidance from DIR and UT System. This HSAIS checklist will be completed for all AI Systems and used to identify HSAIS requiring the enhanced assessment and tracking required by SB 1964.

Responsible Party
Mary Dickerson, Associate Vice President and Chief Information Security Officer

Implementation Date
July 15, 2026

#2 – Approval of AI Systems
Cause Policies have not been updated to reflect the current business process. **Risk** Noncompliance with policy. **Condition** Management informed us the AI Governance Committee (also known as the AI Governance & Policy Subcommittee) is no longer approving AI Systems. **Criteria** Handbook of Operating Procedures (HOOP) 235 Governance and Use of Artificial Intelligence requires all AI Systems to be approved by the AI Governance Committee.
Recommendation Update HOOP 235 to reflect the current business process. **Rating** Medium
Management Response HOOP 235 was created prior to passage of SB 1964 and directives from DIR and guidance from UT System were issued. We are working now to update HOOP 235 to address the current state and UT System requirements as well as to reflect the evolution of university business practices involving AI. **Responsible Party** Mary Dickerson, Associate Vice President and Chief Information Security Officer **Implementation Date** January 15, 2027

We would like to thank the Information Technology, Information Security, and School of Biomedical Informatics staff and management who assisted us during the engagement.



Daniel G. Sherman, MBA, CPA, CIA
Vice President & Chief Audit Officer

OBSERVATION RATINGS

Priority	An issue that, if not addressed timely, has a high probability to directly impact achievement of a strategic or important operational objective of UTHealth or the UT System as a whole.
High	An issue considered to have a medium to high probability of adverse effects to a significant office or business process or to UTHealth as a whole.
Medium	An issue considered to have a low to medium probability of adverse effects to an office or business process or to UTHealth as a whole.
Low	An issue considered to have minimal probability of adverse effects to an office or business process or to UTHealth as a whole.

NUMBER OF PRIORITY OBSERVATIONS REPORTED TO UT SYSTEM

None

MAPPING TO A&AS FY2025 RISK ASSESSMENT

Reference	Risk
N/A	Reliance on AI requires more controls and staffing resulting in increased costs.
N/A	Artificial intelligence is employed without adequate oversight/vetting resulting in a breach.
N/A	Use of artificial intelligence grows at a faster pace than can be monitored or controlled leading to potential data breaches and increased costs.

DATA ANALYTICS UTILIZED

Not applicable

ENGAGEMENT TEAM

VP/CAO – Daniel G. Sherman, MBA, CPA, CIA
Supervisor – Brook Syers, CPA, CIA, CISA, CFE
Lead – Tammy Coble, CISA

END OF FIELDWORK DATE

May 4, 2026

ISSUE DATE

June 9, 2026

REPORT DISTRIBUTION

Audit Committee
Dustan Brennan
Dr. Martin Citardi
Mary Dickerson
Shirlanda Fairley
Dr. Xiaoqian Jiang
Michael Patriarca
Christina Solis
Ana Touchstone
Michael Tramonte
Eric Williams
Amar Yousif
Dr. Jiajie Zhang