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

Inbound Email Security

#HSC25AS0006

EXECUTIVE SUMMARY

Auditing & Advisory Services (A&AS) has completed an assurance engagement of inbound email security. 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

The Abnormal AI (Abnormal) platform is utilized by UTHealth for inbound email security. It integrates with Microsoft 365 and utilizes artificial intelligence to automatically detect and block threats such as phishing, malware, and spam before they reach users' inboxes. By analyzing tens of thousands of behavior signals, it establishes baselines for normal user and vendor activity, allowing for the identification of subtle deviations indicative of malicious activity.

Objectives

Our objective was to determine whether controls around inbound email security are adequate and functioning as intended. Specifically, to determine if:

- Policies and procedures have been established.
- A vendor security risk assessment of Abnormal was performed.
- A SOC 2 report was completed and any significant findings were adequately addressed.
- Agreements have been executed with the vendor and the vendor is TX-RAMP certified.
- Users have appropriate access based on their roles & responsibilities.
- Quarterly access reviews were performed and properly documented.
- Suspicious email reports were analyzed by Abnormal, reviewed by a Security Operations Analyst, and a manual report was submitted to Abnormal (if applicable).
- VIP users are appropriate.
- Monthly reports were reviewed and presented at the monthly IT Security Core Team meetings.
- Abnormal user activity is logged.

Scope Period

August 1, 2024 through July 31, 2025

Conclusion

Overall, controls around inbound email security are adequate and functioning as intended. We noted the following opportunities for improvement:

#	Observation Summary	Risk	Risk Rating
1	There was not an initial or periodic risk assessment performed.	Undetected security risks.	**Medium**
2	A FERPA agreement was not executed with the vendor during the procurement of Abnormal.	Increased financial exposure.	**Medium**

OBSERVATIONS & MANAGEMENT RESPONSES

#1 – Vendor Risk Assessments

Cause
There was not an initial or periodic risk assessment performed.

Risk
Undetected security risks.

Condition
At the time of our procedures, we noted no initial or periodic risk assessments of Abnormal had been performed.

Criteria
ITPOL-039 Cloud Computing Policy requires System Owners to contact IT support staff and the procurement department to initiate the review of and the purchasing of cloud services.

HOOP 175 Roles and Responsibilities for University Information Resources and University Data requires the System Owner to perform a risk assessment annually for Mission Critical Information Resources and biennially for non-Mission Critical Information Resources.

Recommendation(s)
Perform a vendor risk assessment and develop a process to ensure it is performed and documented on a periodic basis going forward.

Rating
Medium

Management Response #1
The Information Security Risk Assessment for Abnormal was completed on August 21, 2025 and made available for A&AS review. The Information Security Risk Management and Consulting team, working in collaboration with Procurement, has defined a process for review and performance of risk assessments for all information technology-related products and services prior to acquisition. The tracking for all assessments and documentation will be maintained in AuditBoard along with scheduled follow-up reassessments determined according to defined risks. A&AS staff has direct access to AuditBoard to view this documentation as needed.

Responsible Party
Mary Dickerson, Associate Vice President and CISO

Implementation Date
August 31, 2025 (to be verified by A&AS)

#2 – FERPA Agreement
Cause A FERPA agreement was not executed with the vendor during the procurement of Abnormal. **Risk** Increased financial exposure. **Condition** At the time of our procedures, we noted a FERPA agreement with Abnormal AI had not been executed. **Criteria** The University of Texas System Board of Regents' Rule 50702 states each U. T. System institution shall adopt a process for the review of all proposed contracts to determine if the services will involve the access of Education Records or Personally Identifiable Information from an Education Record by a third party contractor and contracts should shall include terms that ensure that the contractor will employ FERPA privacy and security safeguards as to all of the institution's Education Records that the contractor will access. Section 6.7 of the ITPOL-039 Cloud Computing Policy requires cloud vendors with access to university data enter into appropriate legal agreements with the university to support HIPAA, FERPA, and any other regulations with which the university is required to comply.
Recommendation(s) Execute a FERPA agreement with Abnormal AI. **Rating** Medium
Management Response #1 The FERPA Agreement for Abnormal AI was executed on August 28, 2025 and made available for A&AS review. The Information Security Risk Management and Consulting team, working in collaboration with Procurement, has defined a process for completion and tracking of applicable agreements and documentation executed for acquisition of information technology-related products and services. The tracking for all documentation will be maintained in AuditBoard. The UTHealth Houston Audit staff has direct access to AuditBoard to view documentation as needed. **Responsible Party** Mary Dickerson, Associate Vice President and CISO **Implementation Date** August 31, 2025 (to be verified by A&AS)

Inbound Email Security

We would like to thank the IT Security and Data Center Operations 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 FY25 RISK ASSESSMENT

Reference	Risk
IT	Failure to confirm vendor certification under TX-RAMP prior to purchase results in acquisition of insecure cloud services
IT	Security risk assessments of software/applications procured through Coupa are not performed prior to implementation, resulting in a breach.
IT	Phishing attacks are successful resulting in a breach.
IT	IT software/hardware is purchased without consideration of integration resulting in increased costs.
IT	Third parties maintain elevated access after contract expiration resulting in inappropriate access.

DATA ANALYTICS UTILIZED
None

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

END OF FIELDWORK DATE
October 10, 2025

ISSUE DATE
October 31, 2025

REPORT DISTRIBUTION
Audit Committee
Richard Anselme
Mary Dickerson
Kevin Dillon
Tony Murry
Ana Touchstone
Amar Yousif