24-203 Windows Server Patching

EXECUTIVE SUMMARY

Auditing & Advisory Services (A&AS) has completed an assurance engagement of Windows server patching. This engagement was performed at the request of the UTHealth Houston (UTHealth) Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

Background
Patches must be applied to Windows Server operating systems to ensure stability, performance, and protection against emerging threats and vulnerabilities. Patches are issued by Microsoft and implemented by Data Center Operations (DCO) and the School of Biomedical Informatics (SBMI) on a monthly schedule.

Objectives/Scope
Our objective was to determine whether controls around Windows Server patching are adequate and functioning as intended. Specifically, to determine if:
- Policies and procedures are in place.
- Change notifications for DCO patches are adequately documented.
- Patches are implemented within 30 (SBMI) or 60 days (DCO).
- Status reports are sent to respective DCO system administrators.
- DCO (weekly) and SBMI (monthly) reports are reviewed by responsible parties.
- DCO server inventory reports are sent on a monthly basis to the IT infrastructure team.
- DCO patches (including emergency patches) are reviewed during Change Board meetings.
- DCO patches are tested prior to implementation.
- SBMI patch alerts are configured in NinjaOne.

Scope Period
June 1, 2024 through November 30, 2024

Conclusion
Overall, controls around Windows Server patching are adequate and functioning as intended. We noted no observations during our procedures.

We would like to thank the DCO and SBMI 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 FY 2024 RISK ASSESSMENT

Reference	Risk
IT-28	Patches/upgrades not applied timely to data center servers/applications/desktops

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 23, 2025

ISSUE DATE
June 2, 2025

REPORT DISTRIBUTION
Audit Committee
Ryan Bien
Mary Dickerson
Kevin Dillon
David Ha
Tony Murry
Ana Touchstone
Amar Yousif
Dr. Jiajie Zhang