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

System Owner Responsibilities

#HSC26AS1050

EXECUTIVE SUMMARY

Auditing & Advisory Services (A&AS) has completed an assurance engagement of System Owner Responsibilities. 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

HOOP 175 Roles and Responsibilities for University Information Resources and University Data (HOOP 175) defines system owners as the person responsible for the business function or project that depends on a system. System owners are responsible for the overall security, compliance, value, continuity, assigning custodians and an Information Security Administrator (ISA), managing access, performing risk assessments, protecting and classifying data, ensuring regulatory compliance, reporting security incidents, overseeing the departmental business continuity (BCP) and disaster recovery plans (DRP), and retaining records in accordance with university policies.

Objectives

Our objective was to determine whether controls over system owner responsibilities are adequate and functioning as intended. Specifically, to determine if:

- Responsibilities outlined in HOOP 175 align with UTS 165 Information Resources Use and Security Policy and are consistently followed.
- Mission critical and critical systems have a designated system owner recorded in the Optro Third-Party Risk Management system (TPRM). Additionally, TPRM records are complete and accurate.

Scope Period

Mission critical and critical systems as of February 23, 2026.

Conclusion

Overall, controls around system owner responsibilities are adequate and functioning as intended. We noted the following opportunities for improvement:

#	Observation Summary	Risk	Risk Rating
1	System owners are not consistently in compliance with the requirements of HOOP 175. Training on the responsibilities of system owners is available but is not required.	Information breach and/or inability to effectively recover from a disaster.	**High**
2	The TPRM does not reflect all system owners and/or does not always contain information of all key fields.	Unclear accountability resulting in	**Medium**

		inadequate system oversight.	

OBSERVATIONS & MANAGEMENT RESPONSES

#1 – System Owner Responsibilities

Cause
System owners are not consistently in compliance with the requirements of HOOP 175. Training on the responsibilities of system owners is available but is not required.

Risk
Information breach and/or inability to effectively recover from a disaster.

Condition
We selected a sample of 20 systems (13 mission critical and 7 critical) and obtained evidence of BCPs/DRPs, quarterly access reviews, security incident reporting, third-party assessments, and data retention practices. We noted five systems were not in production at the time of our review. For the remaining 15 systems, we noted the following issues (with some overlap):

Number of Systems	Exception
12	BCP not documented and/or available for review.
10	Most recent user access review not performed, available, and/or documented.
8	DRP not documented and/or available for review.
5	Records retention and disposal practices (e.g., system data, external reports, user access reviews) not documented and/or made available for review.
2	Third-party risk assessment not completed within the required timeframe.

Additionally, at the time of our procedures, we noted the system owner webpage did not reflect all responsibilities under HOOP 175. It was subsequently corrected.

Criteria
HOOP 175 outlines system owner responsibilities around delegation, assignment of custodians/ISAs, system value, risk assessments, classification/security of data, security control exceptions, system access reviews, training, BCP/DRP plans, and records retention.

Recommendation(s)
Management should assess how system owner responsibilities are communicated and managed, including oversight and assurance functions to ensure adequate process controls and data protection are developed and maintained.

Rating
High

Management Response #1
We agree that there can be more effective communications with designated System Owners regarding their responsibilities. To achieve this, we are implementing the following:

1. The System Owner Program training has recently been revised and video recorded. The recording will be shared with all currently designated System Owners (SO) and Information Security Administrators (ISA).
2. Along with the recorded training, a SO Responsibilities summary sheet is being created and will be distributed to the SO and ISAs.

System Owner Responsibilities

3. Upon designation, all new SO and ISAs will be provided with the video training and responsibilities sheet.
4. At least annually, all SO and ISA will need to send an acknowledgment/confirmation to Information Security that they have reviewed the training video and understand their responsibilities. Receipt of this acknowledgement will be tracked in Optro.

We are also investigating the possibility of adding a training requirement to HOOP 175 as a mandatory requirement of SOs and ISAs.

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

Implementation Date
October 15, 2026

#2 Missing and/or Incomplete Records
Cause The TPRM does not reflect all system owners and/or does not always contain information of all key fields. **Risk** Unclear accountability resulting in inadequate system oversight. **Condition** As of February 23, 2026, there were a total of 122 systems designated as mission critical or critical in TPRM. We noted 17 systems and one test system that did not have a system owner assigned in TPRM. Management informed us the missing system owner assignments may be due to the initial data import during the TPRM implementation. In two cases, we noted the system owner listed was inaccurate. Additionally, we noted instances of incorrect and/or blank fields for custodians, ISAs, business impact, most recent risk assessment date, and risk assessment frequency. **Criteria** Each information system is required to have an assigned system owner who must fulfill the 14 required responsibilities as outlined in HOOP 175.
Recommendation(s) Develop and implement an oversight process to ensure system owner assignments are accurate and required record fields are completed in TPRM. **Rating** Medium
Management Response #1 We agree that not all of the fields in TPRM were completed as the information for each System was populated in Optro. We have since undertaken an extensive review of all of the active Systems currently tracked in Optro to confirm that all applicable fields are completed. We have also implemented a Quality Assurance process upon System intake to verify that all applicable fields are completed before the System is designated as Active. Finally, we are working with the other university area experts outside of Information Security with data tracked in Optro to ensure their fields are completed as applicable. **Responsible Party** Mary Dickerson, Associate Vice President and Chief Information Security Officer **Implementation Date** October 15, 2026

System Owner Responsibilities

We would like to thank the IT Security, Risk Management & Consulting 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 FY2026 RISK ASSESSMENT

Reference	Risk
IT 5	User access reviews are not performed on a regular basis resulting in a breach.
IT 30	System owners do not perform their duties resulting in a breach.

DATA ANALYTICS UTILIZED
None

ENGAGEMENT TEAM
VP/CAO – Daniel G. Sherman, MBA, CPA, CIA
Supervisor – Kathy Tran, CIA, CISA, CISSP, CFE, CGAP
Lead – Shara Vialva, CIA, CPA

END OF FIELDWORK DATE
May 14, 2026

ISSUE DATE
June 9, 2026

REPORT DISTRIBUTION

Audit Committee	Rose Hochner	Ana Touchstone
Richard Anselme	Jennifer Huenemeier	Amar Yousif
Mary Dickerson	Michael Patriarca	