UTHealth
The University of Texas
Health Science Center at Houston

16-117 and 16-207 ITAMS Integrated Audit

We have completed our audit of the IT Asset Management System. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

As a result of a prior audit finding, the IT Asset Management System (ITAMS) was developed internally by UTHealth to track information technology (IT) equipment within a central data repository. In 2014, IT equipment (including computers, laptops, USB drives, smartphones, tablets, and certain peripheral equipment) tracked in spreadsheets by individual departments and schools was loaded into ITAMS. ITAMS also tracks status (active/inactive/lost/missing/stolen/surplus), encryption information, ownership, and location. UTHealth usernames and passwords are used to access ITAMS and there are no current automated interfaces with any other applications.

OBJECTIVES

The objective of this audit was to determine whether the controls over IT asset management and the ITAMS application are adequate and functioning as intended.

SCOPE PERIOD

The scope period includes ITAMS inventory records as of September 2016.

METHODOLOGY

The following procedures were performed:

- Obtained and reviewed institutional and local policies and procedures around the inventory process for IT equipment.
- Obtained a download of all active IT equipment, selected a random sample, observed each piece of equipment in the field, and verified data in ITAMS was accurately recorded. Additionally, verified equipment data in the Capital Asset Management (CAM) inventory application was accurately recorded (where applicable).
- Randomly selected a sample of IT equipment and verified each piece of equipment was recorded in ITAMS (and the CAM inventory application, where applicable).
- Selected a random sample of lost, missing, or stolen IT equipment and verified appropriate forms were completed and filed. For stolen IT equipment, verified a police report was filed with UT Police (UTP-H).
- Obtained the ITAMS access listing and verified that access was appropriate and commensurate with job responsibilities. Selected a random sample of users and verified access was approved via a ticket or email request to the appropriate approvers.

713.500.3160 phone 713.500.3170 fax
P.O. Box 20036
Houston, Texas 77225
www.uthouston.edu

- Conducted an electronic data analysis to identify missing information, duplicate records, and other inconsistencies in the ITAMS database. The results were shared with IT so ITAMS policies and procedures could be developed to address our observations.

AUDIT RESULTS

A&AS identified areas of improvement related to incorrect/missing data, the reporting of lost/missing/stolen equipment, policies and procedures, and access to the ITAMS application:

- ITAMS policies and procedures have not been developed, approved, and implemented.
- In many cases, equipment data in ITAMS are incorrect and/or missing.
- Lost/missing/stolen equipment are not consistently reported to Finance, IT Security, and UTP-H.
- Policies and procedures for granting access to ITAMS have not been developed, approved, and implemented.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None.

We would like to thank the staff and management within UTHealth IT General Administration (GADM), McGovern Medical School Information Technology (MSIT), Clinical Technology, Harris County Psychiatric Clinic (HCPC), School of Public Health (SPH), School of Biomedical Informatics (SBMI), Network Operations, and Treasury Management, who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

MAPPING TO FY 2016 RISK ASSESSMENT

Risk (Rating)	Risk #13 Networking equipment is not periodically updated to new technologies and standards. Risk #43 Deferred maintenance of research and other equipment. Risk #47 Leasing is used to circumvent procurement policies and limits. Risk #96 Equipment leasing contracts are not structured for cost efficiency.

DATA ANALYTICS UTILIZED

Data Analytic #1	Obtained a download file of all ITAMS data and identified anomalies and/or inconsistencies using data analytics software.

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA

Audit Manager	Brook B. Syers , CPA, CIA, CISA, CFE
Auditor Assigned	Lieu Tran, CISA
End of Fieldwork Date	February 2, 2017
Issue Date	March 20, 2017

Copies to:
Audit Committee
Michael Tramonte
Richard Miller
Amar Yousif
Bassel Choucair
Derek Drawhorn
Kevin Granhold
Dr. James Griffiths
Madhavkrishna Sankhavaram
Ryan Bien

Issue #1

Texas Government Code Section 403.272(b) specifies that all personal property owned by the state shall be accounted for by the agency that possesses the property.

UTS165 Information Resources Use and Security Policy (section 3.2 Information Security Program) requires each Security Program to document the current inventory of institution-owned or managed computing devices deployed throughout the institution.

A&AS noted ITAMS policies and procedures have not been developed, approved, and implemented. Additionally, A&AS requested and reviewed the local policies and procedures around inventory for seven schools/areas across UTHealth and noted inconsistencies around the performance of periodic inventories and other guidance.

A&AS noted that each organization utilizes different practices and taxonomy for recording equipment in ITAMS. Certain organizations inventory and track peripherals (such as monitors/printers), while other organizations do not. Equipment is generally identified by serial number, MSIT, CAM, or GADM tag, or a combination thereof.

ACCURACY OF INVENTORY

A&AS obtained a download file of all information in ITAMS as of September 2016. To verify the accuracy of active equipment data in ITAMS, A&AS selected a random sample of 25 and conducted field observations. The following was noted:

Finding	# of Equipment	% of Sample
No department or sub-department recorded	11	44%
No owner recorded	5	20%
Incorrect status	5	20%
Incorrect or missing campus, building, or location	2	8%
No explanation recorded to support change in status (active to lease returned)	2	8%
Multiple serial numbers recorded	1	4%
CAM tag number or UTHealth identification number not recorded	1	4%

	COMPLETENESS OF INVENTORY To verify the completeness of inventory in ITAMS, A&AS selected a sample of 28 pieces of IT equipment in the field and verified each was recorded in ITAMS. There were no exceptions noted.
Recommendation #1	We recommend a policy and procedure be developed, approved, and implemented that addresses required data fields in ITAMS and ensures the accuracy of IT equipment records.
Rating	Medium
Management Response	We will develop, approve, and implement an IT policy and procedure that addresses required data fields in ITAMS and ensures the accuracy of IT equipment records.
Responsible Party	Rick Miller & Bassel Choucair
Implementation Date	August 31, 2017

Issue #2	*The CAM Handbook (Section J: Lost or Stolen Equipment)* requires the following in cases where property is missing or stolen: • The chair or designated administrative official must complete a *Missing, Damaged or Stolen Property Report Form (OAG 74-194)* and report to the Property Manager, or AVP of Finance. • If stolen, UTP-H must be immediately notified so an investigation can be conducted and an offense/incident report completed. *ITGD-001 Laptop Security Guidelines* require the following for missing or stolen laptops: • The department manager should contact and report missing equipment to the UTP-H. • Department manager should notify the local IT support staff and the IT Security department when equipment is lost or stolen. • The department manager should complete and submit the *Missing or Stolen Equipment Form (ITF-004)* A&AS obtained a download file of all information in ITAMS as of September 2016. We identified 100 lost, missing, or stolen equipment and selected a random sample of 10 to verify appropriate forms (OAG 74-194 or ITF-004) were filed and UTP-H was notified (for stolen equipment only). The following issues were noted: • 4 lost or stolen pieces of equipment were not reported to IT Security. • 3 pieces of equipment had the incorrect status noted in ITAMS. . • 2 pieces of equipment did not have the UTP-H report number documented in ITAMS. • 2 pieces of equipment were not reported using the OAG 741-94 and/or ITF-004 forms. • 1 piece of equipment was not reported to UTP-H as stolen.
Recommendation #2	In addition to developing a policy and procedure for ITAMS (see Recommendation #1), we recommend refresher training be conducted to reemphasize the requirements around lost/missing/stolen IT equipment.
Rating	Medium
Management Response	In addition to developing an IT policy and procedure for ITAMS at Recommendation #1, we will conduct a refresher training and/or communication to reemphasize the requirements around lost/missing/stolen IT equipment.
Responsible Party	Rick Miller & Bassel Choucair

Implementation Date	August 31, 2017

Issue #3	*UTS165 - Standard 4: Access Management:* *4.1 Access Management* – requires all institutions to adopt access management processes to ensure that access to information resources is restricted to authorized users. *4.2 Access Management Process* – requires: (d) reviewing, removing and/or disabling accounts at least quarterly, or more often if warranted by risk, to reflect current user needs or changes of user role or employment status; (e) expiring passwords or disabling accounts based on risk. A&AS obtained the user access listing from ITAMS and verified access was appropriate and commensurate with job responsibilities. We noted one user with administrator privileges who was also a member of the ITAMS development team (separation of duties issue). A&AS verified that the administrator access was removed during fieldwork. Additionally, we inquired about the approval process for accessing ITAMS and were informed that access is typically approved via HEAT Ticket or email request to the Lead Administrator and/or Data Owner at each school/organization. We selected a random sample of 20 users across schools/organizations to test this requirement. We noted the following issue: • 17 of 20 users (85%) did not have their access approved via a HEAT ticket or email request to the ITAMS Lead Administrator and/or Data Owner at each school/organization.
Recommendation #3	We recommend a policy and procedure be developed, approved, and implemented that addresses the process for ITAMS access, including the required approvals and documentation.
Rating	Low
Management Response	We will develop, approve, and implement an IT policy and procedure that addresses the process for ITAMS access, including the required approvals and documentation.
Responsible Party	Rick Miller & Bassel Choucair
Implementation Date	August 31, 2017