UTHealth
The University of Texas
Health Science Center at Houston

16-116/206 Identity Management Integrated Audit

We have completed our audit of Identity Management. 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

UTHealth maintains a fully automated provisioning system to control the identity life-cycle. With this automated system, UTHealth is able to provide each affiliated person with a unique ID that is used to centrally provision and control access to its online resources.

Before a unique ID is issued, the identities of all users must be verified via official hiring or acceptance procedures. In order to maintain affiliation with the U.T. System Identity Management Federation, UTHealth implemented Level of Assurance 2 (LOA2) registration and identity proofing requirements throughout the organization.

OBJECTIVES

The objective of this audit was to determine whether controls over ID proofing and issuing credentials to students, employees, and guests are appropriate and functioning as intended.

SCOPE PERIOD

The scope period was September 1, 2014 – August 31, 2015

METHODOLOGY

The following procedures were performed:

- Verified formal policies and procedures concerning ID proofing and issuing credentials exist and are reviewed annually.
- Reviewed a sample of U.S. (25) and foreign (25) employees' I-9 forms used to verify identity and employment eligibility and inspected for compliance with United States Citizenship and Immigration Services (USCIS) guidelines.
- Selected a sample of U.S. (25) and foreign (25) students from a combination of schools and inspected evidence of identity verification, confirmed vetting by an authorized Registration Agent or Student Affairs personnel, and verified clearance from the Office of International Affairs (OIA) was obtained for foreign students.
- Selected a sample of U.S. (25) and foreign (25) guests and inspected evidence of identity verification, confirmed vetting by authorized Registration Agents, and verified clearance from OIA was obtained for foreign guests.
- Reviewed a sample of Registration Agents (5) and Credentialing Agents (10) to confirm appropriate approvals were obtained prior to appointment and training was administered.

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

AUDIT RESULTS

A&AS identified areas of improvement related to Registration Agents (RA), Credentialing Agents (CA), and identity verification:

- The policies and procedures around identify proofing and the issuance of credentials have not been updated to reflect the current business practices.
- Addresses and a second ID for guests are not recorded/inspected.
- The identity verification of students is not consistently documented.
- The training of RAs is not documented.
- Procedures for appointing CAs and granting access to the user administration tool have not been defined.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None

We would like to thank the staff and management within IT Security, Human Resources, and the Office of Student Affairs within each school who assisted us during our review.

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

MAPPING TO FY 2016 RISK ASSESSMENT

Risk (Rating)	R.17 A guest account could be used to infiltrate the UTHealth network and plant malware or steal data. R.56 Unfederated authentication access granted by partners and UThealth does not cease when an employee is terminated. R.65 The identity verification of foreign remote students is not performed. R.83 Online students' exams and coursework are completed by others.

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, IT Audit Manager
Auditor Assigned	Brittney Alexander, IT Auditor
End of Fieldwork Date	March 28, 2016
Issue Date	April 19, 2016

Copies to:
Audit Committee
Amar Yousif
Eric Fernette

Issue #1	<u>GUESTS</u> ITSOP-011 *Identity Proofing and Credential Issuance* (ITSOP-011) Section 6.2.7 requires two forms of identification (ID) to be inspected by the RA for sponsored guests, including both U.S. citizens and foreign nationals. An ID number, address, and date of birth are required to be recorded for the first ID, as well as the ID number for the second. Additionally, ITSOP-011 states: "All UTHealth visitors who are foreign nationals on a nonimmigrant visa status are expected to obtain clearance from OIA prior to joining UTHealth in any capacity (paid or unpaid short or long-term, full time or part time, faculty or classified) and in any role, including observers, visiting scientists, degree and non-degree students, researchers, trainees, and employees." We selected a sample of 25 sponsored U.S. citizen guests, noting there was no evidence that an address was recorded or a second ID inspected for any of the guests in our sample. Additionally, we selected a sample of 25 foreign national guests, noting there was no evidence that an address was recorded, a second ID was inspected, or clearance was obtained from OIA for any of the guests in our sample. The CISO informed us that foreign national guests are not required to obtain OIA clearance and that ITSOP-011 has not been updated to reflect this practice. We noted that OIA clearance is an internal procedure for foreign nationals and is not required for LOA2. Additionally, an inconsistency in ITSOP-011 was noted. Section 6.2.7 states that two forms of ID are required to be provided for inspection, while Section 6.3 states that only one form of ID is required. <u>STUDENTS</u> ITSOP-011 requires the RA to maintain a record of each student whose identity has been verified and the steps taken to verify his/her identity, including the evidence required (e.g. driver's license number or passport number). A&AS selected a sample of 25 foreign national students and 25 U.S. citizen students from a combination of the schools and requested evidence of identity verification. Evidence of identity verification could not be located for : • 22 of 25 (88%) US citizen students • 15 of 25 (60%) foreign national students
Recommendation #1	We recommend that IT Security review the current identity proofing and credentialing process and update ITSOP-011 accordingly. Additionally, we recommend that training be provided to reinforce the documentation

	requirements and periodic quality checks be conducted as needed to ensure the requirements are being met.
Rating	Medium
Management Response	We agree with the recommendation. We will review and update all IDM policies to bring them in line with the UT System federation guidelines, as well as provide training and conduct periodic quality checks as deemed necessary. Any IDM policy changes required as part of UT System federation guidelines could result in the need to reconfigure fields in the UserAdmin application, which could increase the time needed to meet this recommendation.
Responsible Party	Amar Yousif
Implementation Date	October 31, 2016

Issue #2	ITSOP-009 *Registration Agent Appointment and Revocation* (ITSOP-009) states that an RA must complete training and sign a Roles and Responsibilities form prior to appointment. A&AS selected a sample of five RAs and requested the Roles and Responsibilities Form and evidence of training. For 5 out of 5 (100%) RAs in our sample, neither the Roles and Responsibilities form nor evidence of training could be located. The RA Coordinator informed us that the Roles and Responsibilities Form is no longer used.
Recommendation #2	We recommend IT Security review the current process for RA training and update ITSOP-009 accordingly. Additionally, we recommend IT Security maintain evidence that RAs have been properly trained.
Rating	Medium
Management Response	We will review the current process for RA training and update ITSOP-009 accordingly. We will maintain evidence of RA training going forward and explore the possibility of using LMS to maintain proof/documentation of training.
Responsible Party	Amar Yousif
Implementation Date	October 31, 2016

Issue #3	A Credentialing Agent (CA) is an individual authorized to issue the user's credentials to UTHealth's network (once their identity has been verified), as well as issue and reset passwords. Formal policies/procedures are not in place for appointing CAs; however, the IDM Manager at the time of our fieldwork informed us that a prospective CA must have access requested/approved by their manager and attest to having reviewed the Password Policy and Password Reset SOP documents. A&AS selected a sample of 10 CAs from the User Administration Tool access listing, from which CAs issue credentials. We requested documentation to support approval and attestation according to the stated process. For 10 of 10 (100%) CAs in our sample, evidence of approval and attestation could not be located.
Recommendation #3	We recommend IT Security develop and implement procedures for appointing Credentialing Agents and granting access to the user administration tool.
Rating	Medium
Management Response	We agree with the recommendation and will develop and implement procedures for appointing CAs and granting access to the UserAdmin application. We will explore the possibility of using LMS to facilitate this process.
Responsible Party	Amar Yousif
Implementation Date	October 31, 2016