Office of Internal Audit

UTSouthwestern
Medical Center

System Accessibility Audit

Internal Audit Report 19:23

June 7, 2019

Table of Contents

Detailed Observations and Action Plans Matrix

Background

The University of Texas Southwestern Medical Center is committed to ensuring that systems and websites that are either procured through a third party vendor or developed by UT Southwestern, are accessible to everyone, including individuals with disabilities, in compliance with the requirements of the Americans with Disabilities Act (ADA). State regulations for compliance with the ADA are promulgated through Texas Administrative Code (TAC) and rules set forth by the Texas Department of Information Resources (DIR). UT System Policy 150 Accessibility Compliance requires all UT institutions to comply with DIR rules.

The DIR rules define Electronic and Information Resources (EIRs), which are required to be accessible. EIRs include a wide variety of digital technologies including telecommunications products, information kiosks, transaction machines, websites, multimedia, digital signage and office equipment. The rules also require each state agency to designate an Accessibility Coordinator responsible for ensuring accessibility compliance.

At UT Southwestern, the Accessibility Coordinator position has been designated as a manager in Academic and Administrative Information Resources (AAIR) – Web Services department. However, processes to achieve system accessibility compliance involve coordination among several functions across the Medical Center including Supply Chain Management, Information Resources and Communications, Marketing and Public Affairs (CMPA). These compliance processes are further complicated by the decentralized nature of system acquisition and web site development. For example, web site development is performed by AAIR Operations - Web Services, CMPA, as well as certain departments. See Appendix B for an illustration of the roles and responsibilities of these functions as well as the overall governance bodies required by the DIR rules.

Scope and Objectives

The Office of Internal Audit has completed its System Accessibility audit. This was a risk based audit and part of the fiscal year 2019 Audit Plan. The audit scope period included activities from January 2018 to current. The review included systems and websites that could be accessed through the Internet, collectively referred to as public-facing. Audit procedures included interviews with stakeholders, review of policies and procedures and other documentation, substantive testing, and data analytics.

The overall objective for the System Accessibility Audit was to determine the Medical Center's compliance with the Americans with Disabilities Act (ADA) related to accessibility features of key systems and web sites.

We conducted our examination according to guidelines set forth by the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Detailed Observations and Action Plans Matrix

Conclusion

Overall, there are several key opportunities to improve processes in place to ensure compliance with accessibility requirements for key systems and websites in use at UT Southwestern. A centralized governance structure is needed to provide oversight and implement an accessibility compliance plan. Monitoring for the appropriateness of user access is also needed for the Siteimprove Accessibility Tracker software used to identify web site accessibility errors, as well as the Insite Content Management System used to maintain content for the patient-facing web site, UTSWMed.org.

Included in the table below is a summary of the observations noted, along with the respective disposition of these observations in accordance with the Medical Center internal audit risk definitions and classifications See Appendix A for Risk Rating Classifications and Definitions.

This report is divided in two sections to assist management in identifying those opportunities for improvement of interest for each respective constituency: Academic and Administrative Information Resources (AAIR) and Communications, Marketing and Public Affairs. These opportunities are summarized below:

Strengths identified during the audit include:

- Contracts Management ensures system accessibility language is included in all contracts for electronic information resources
- Siteimprove Accessibility Tracker software is used to scan websites for system accessibility compliance

The improvement opportunities identified for AAIR Operations – Web Services are summarized below.

Priority (0)	**High (1)**	**Medium (1)**	**Low (1)**	**Total (3)**

● **Establish a Formalized Structure for Oversight of Compliance with System Accessibility Regulations –** Several governance-related elements including an Accessibility Coordination Team, Accessibility Compliance Plan and institutional policy are not in place to provide effective oversight and ensure compliance with the system accessibility rules.

● **Enhance Procedures for Siteimprove Access –** Procedures are not in place for removing access to the Siteimprove Accessibility Tracker software when users terminate or transfer and current licensing is not adequate to scan all known website pages.

● **Develop Online Web Content Creator Refresher Accessibility Training –** Online refresher training to remind or update developers on current accessibility and usability requirements is not available.

Detailed Observations and Action Plans Matrix

The improvement opportunities for Communications, Marketing and Public Affairs are summarized below.

Priority (0)	High (1)	Medium (1)	Low (0)	Total (2)

- ● **Implement Monitoring Procedures and Document User Access Maintenance Procedures for the Insite Content Management System –** Procedures are not in place to periodically monitor the appropriateness of Administrator access granted to the vendor's employees to the Insite Content Management System (CMS). Additionally, procedures to maintain user access for UT Southwestern employees were not formally documented.
- ● **Improve Procedures for Website Accessibility Error Remediation –** Procedures for remediating errors identified by Siteimprove do not include steps to track, follow up and escalate errors to ensure they are remediated to ensure compliance.

Management has plans to address the issues identified in the report and in some cases has already implemented corrective actions. These responses, along with additional details for the improvement opportunities listed above are included in the Detailed Observations and Action Plans Matrix (Matrix) section of this report.

We would like to take the opportunity to thank the departments and individuals included in this audit for the courtesies extended to us and for their cooperation during our review.

Sincerely,

Valla F. Wilson, Vice President, Chief Audit Executive/Interim Chief Compliance and Privacy Officer

Audit Team:
Gabriel Samuel, Senior IT Auditor
Jeff Kromer, Director, IT & Specialty Audit Services

cc: Jacquelyn Clark, J.D., Attorney, Legal Affairs
Charles Cobb, Associate Vice President, Supply Chain Management
Shawn Cohenour, Director, Contracts Management
Arnim E. Dontes, Executive Vice President, Business Affairs
Travis Gill, J.D., Director Institutional Equity and Accessibility
Joel Johnson, Assistant Vice President, Digital and Interactive Engagement
Sherleen Mahoney, Digital Communications Strategist, Digital and Interactive Engagement
Tom Mathews, Director Interactive Media & Web Services, IR-AAIR Operations
Jonathan Maedche, Manager Information Resources, IR-AAIR Operations
Marc E. Milstein, Vice President, Information Resources & Chief Information Officer
Heather Mishra, Associate Vice President, Academic & Administrative Information Systems
Marc A. Nivet, Ed.D., Executive Vice President, Institutional Advancement
Adolfo Ortuzar, Director, IR-Academic & Administrative IR Operations
Paige Poletes, Assistant Director, Digital Engagement, Digital and Interactive Engagement
Nathan Routen, Interim Chief Information Security Officer
Joshua Spencer, Associate Vice President & Chief Technology Officer
Thomas Spencer, Ph.D., Assistant Vice President, IR Operations and Compliance, Academic and Administrative Information Resources
Valla F. Wilson, Associate Vice President, Chief Audit Executive/Interim Chief Compliance and Privacy Officer

AAIR Operations - Web Services Observations

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: High ● 1. **Establish a Formalized Structure for Oversight of Compliance with Systems Accessibility Regulations** Several governance-related elements are not in place to provide effective oversight and ensure compliance with the system accessibility rules: • An Accessibility Coordination Team for EIR Remediation (ACTER) has not been established to be given all authority and resources necessary to develop and implement policies, procedures, and reporting to implement an Accessibility Compliance Plan across UT Southwestern. • An Electronic Information Resource (EIR) Accessibility Compliance Plan has not been documented as required by TAC. • A formal institutional accessibility policy has not been established as required by Texas Administrative Code (TAC) Section 206.7. The UT System Office of General Council has issued a bulletin, which serves as a system-wide accessibility policy, but that is not specific to the Medical Center's environment. • A comprehensive inventory of all institutional websites and systems required to be accessible has not been compiled to assist in measuring the extent of remediation necessary. A spreadsheet with certain websites and accessibility testing exists, but is not comprehensive and omits systems.	1. Establish an Accessibility Coordination Team for EIR Remediation (ACTER) to be given all authority and resources necessary to develop and implement policies, procedures, and reporting to implement the Accessibility Compliance Plan across UT Southwestern. To ensure an effective cross-functional plan is developed, include in the ACTER, at least, representatives from Compliance, Legal, Diversity, Inclusion and Equal Opportunity, Information Security, Information Resources, Supply Chain Management, Contracts Management and Communications, Marketing & Public Affairs 2. Document a formal Accessibility Compliance Plan with goals for making EIR accessible, progress measurements towards meeting those goals and the process for corrective actions. 3. Submit for approval a formal institutional policy for System Accessibility outlining the roles and responsibilities of the EIR Accessibility Coordinator, the Accessibility Coordination Team and procedures to be followed to implement the institution's Accessibility Compliance Plan as recommended in #2 above. 4. Compile a comprehensive inventory of all institutional websites and systems required to be accessible.	**Management Action Plans:** 1. Form Accessibility Coordination TEAM (ACTER) with representatives as recommended. 2. Coordinate with the ACTER to document a formal Accessibility Compliance Plan 3. Coordinate with the ACTER to develop and submit for approval a formal institutional policy for System Accessibility. 4. Compile a comprehensive inventory of all websites and systems required to be accessible. **Action Plan Owners:** Assistant Vice President, IR Operations and Compliance Director, Interactive Media and Web Services **Target Completion Dates:** 1. September 30, 2019 2. September 30, 2019 3. October 31, 2019 4. August 31, 2019

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium 🟡 2. **Enhance Procedures for Siteimprove Access** Procedures are not in place for maintaining access to the Siteimprove Accessibility Tracker software when users terminate or transfer and current licensing is not adequate to scan all known website pages. Testing revealed 31 users who retained access after they terminated from the institution. Since these user accounts are independent of their network IDs, they could still be used after termination, However, risk is not considered high since their access permits them only to clear existing error messages in their queue and they cannot maintain web content. These users were immediately removed upon notice from Internal Audit. The Siteimprove Accessibility Tracker software is used to scan, within licensing limits, all known UT Southwestern websites for accessibility and other usability errors. Current licensing for this software limits scanning to 20,000 pages, which is not adequate to scan all pages for known UT Southwestern websites. As a result, some accessibility or other usability errors may exist that are not detected, resulting in increased compliance and reputational risk.	1. Implement and document a process to periodically review access to the Siteimprove software for users that have terminated or transferred to prevent unauthorized access. 2. Regularly obtain listings of terminated or transferred users from the PeopleSoft HCM system (similar to that used by the System Access Management group) and scan to determine whether access to Siteimprove should be disabled for any users on the listings. 3. Since email addresses may be similar, consider using a field available in Siteimprove to store the UT Southwestern network ID of each user. 4. In coordination with the Siteimprove vendor, explore the feasibility of implementing Lightweight Directory Access Protocol (LDAP), Shibboleth, or a similar technology that would authenticate the user by association with their UT Southwestern User ID. This would reduce the risk of unauthorized access for terminations and transferred users as their access would be disabled automatically. 5. Ensure adequate licensing of Siteimprove to enable scanning of all known web site pages.	**Management Action Plans:** 1. Implement and document monthly review process for terminated and transferred Siteimprove user monitoring. 2. Obtain monthly listings of terminated and transferred users from PeopleSoft HCM. 3. Input Network User ID in the Tag field in Siteimprove for all users. 4. Coordinate with the vendor to evaluate the feasibility of implementing LDAP or a similar technology. Evaluate within 30 days, implement by 60 days after that. 5. a. Obtain pricing for complete coverage by Siteimprove. b. Submit for budget approval. **Action Plan Owners:** Assistant Vice President, IR Operations and Compliance Director, Interactive Media and Web Services **Target Completion Dates:** 1. August 31, 2019 2. August 31, 2019 3. Evaluation - August 31, 2019 Implementation - October 31, 2019 4. August 31, 2019 5. a. August 31, 2019 b. September 30, 2019

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Low ● 3. **Develop Online Web Content Creator Refresher Training for Accessibility** Training for departmental web developers is available in live format, which is primarily intended for new web developers. However, online refresher training to remind or update developers on current accessibility and usability requirements is not available.	Consider developing online refresher training for web developers to remind or update them on current accessibility requirements and institutional policies and standards.	**Management Action Plans:** Develop refresher training for distribution through Taleo online learning environment. **Action Plan Owners:** Assistant Vice President, IR Operations and Compliance Director, Interactive Media and Web Services **Target Completion Dates:** November 30, 2019

Communications, Marketing and Public Affairs Observations

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: High ● 4. **Implement Monitoring Procedures and Document User Access Maintenance Procedures for the Insite Content Management System** Procedures are not in place to periodically monitor vendor access to the Insite Content Management System (CMS) to ensure they are active employees. In addition, procedures to maintain user access to the CMS for UT Southwestern employees were not formally documented at the time of the audit. The Insite CMS is a cloud-based third-party system used to maintain content on the UTSWMed.org patient-facing website. The vendor's employees have Administrator access to the CMS, which grants unlimited access to the system and website content as required to support the system and maintain the user accounts for their employees. This presents a high risk of unauthorized modification of UT Southwestern website content if these users retain access after termination from the vendor. The UT Southwestern Assistant Director of Digital Engagement maintains UT Southwestern accounts for faculty and other departmental employees who design their own web content on the website. Without formal documentation of the procedures for maintaining user access to the CMS, this information may not be available for training of backup or replacement personnel.	1. Implement procedures to periodically obtain listings of active Insite employees to ensure access to the UTSWMed.org website is appropriate. 2. Complete formal documentation of the user maintenance and monitoring procedures for the Insite CMS.	**Management Action Plans:** 1. Obtain monthly listings of active Insite employees assigned to UT Southwestern account and validate access is appropriate. 2. Complete formal documentation of Insite CMS user maintenance and monitoring procedures. **Action Plan Owners:** Assistant Vice President, Digital and Interactive Engagement Assistant Director, Digital Engagement, Digital and Interactive Engagement **Target Completion Dates:** 1. August 31, 2019 2. August 31, 2019

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● 5. **Improve Procedures for Website Accessibility Error Remediation** Procedures for remediating errors identified by Siteimprove do not include steps to track, follow up and escalate errors to ensure they are fixed appropriately to mitigate the risk of litigation and noncompliance with accessibility requirements. The Siteimprove Accessibility Tracker software is used to scan, within licensing limits, all known UT Southwestern websites for accessibility and other usability errors. Departmental websites are maintained by various departmental web content developers, who are responsible for remediating their own errors as reported by Siteimprove.	Enhance Siteimprove error remediation procedures to include tracking, trending and escalation of errors identified. This will ensure errors are remediated timely and appropriately to mitigate risk of litigation and noncompliance with accessibility requirements. Additionally, use the trending data to identify the need for developer training due to repeat or high-volume errors.	**Management Action Plans:** Implement tracking, trending and escalation procedures for Siteimprove error resolution. **Action Plan Owners:** Assistant Vice President, Digital and Interactive Engagement Digital Communications Strategist, Digital and Interactive Engagement **Target Completion Dates:** September 30, 2019

Appendix A – Risk Classifications and Definitions

As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our review. The following chart is intended to provide information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

Risk Definition- The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	**Degree of Risk and Priority of Action**	
	Priority	An issue identified by Internal Audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.
	High	A finding identified by Internal Audit that is considered to have a high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	Medium	A finding identified by Internal Audit that is considered to have a medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action is needed by management in order to address the noted concern and reduce the risk to a more desirable level.
	Low	A finding identified by Internal Audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action should be taken by management to address the noted concern and reduce risks to the organization.

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the subsequent pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions. It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

Appendix B – System Accessibility Roles and Responsibilities

Electronic and Information Systems Accessibility Coordinator

- Establishes Accessibility Coordination Team for EIR Remediation
- Develops Accessibility Policies

Accessibility Coordination Team for EIR Remediation (ACTER)

- Designs and implements EIR identification procedures
- Develops corrective action procedure to bring EIR to compliance
- Develops and maintains procedures to periodically monitor progress made in remediating non-compliant EIR.

Supply Chain and Contracts Management

- Reviews departmental requirements for system acquisition or renewal of contract

-Evaluates system requests for accessibility requirements

-Routes contracts to ISAC for review

-Executes contracts with accessibility language included

Information Systems Acquisition Committee (ISAC)

-Reviews requested systems for security and compliance

-Ensures request is documented appropriately in ServiceNow

-Approves system acquisition and/or renewal

AAIR Operations – Web Services

-Supports certain systems and tools used for web site design and accessibility scanning

-Maintains system access for tools and software for web site design

-Conducts periodic training for web developers

Communications, Marketing and Public Affairs (CMPA)
-

-Receives requests for new websites

-Creates structures and channels for web content

-Partners with Web Services to train content creators

-Ensures departments remediate Siteimprove scanning errors

Departments

-Acquire systems

-Create web content on main UTSW sites.

Develop certain public-facing websites. Examples include:

-UTSW Research Labs

-Peter Ly Lab

-Jewell Lab

-Transplant Physicians

-Focus on Faculty

-Children's Research Institute