

**UT Southwestern**  
Medical Center

**Texas Administrative Code §202  
Compliance Audit**

**Internal Audit Report 17:25**

**September 14, 2017**

# Table of Contents

---

|      |   |   |
|------|---|---|
| I.   | Executive Summary                                   | 3 |
|      | · Background/Scope and Objectives                   | 3 |
|      | · Conclusion  | 3 |
| II.  | Detailed Observations and Action Plans Matrix       | 6 |
| III. | Appendices  | 9 |
|      | · Appendix A – Risk Classifications and Definitions | 9 |

# Executive Summary

---

## **Background**

Created in 1977 by the Texas Legislature, the Texas Administrative Code (TAC) is a compilation of all rules for administering Texas state agencies. The portion of the code applicable to UT Southwestern for purposes of this audit is Title 1 Administration, Part 10 Department of Information Resources, Chapter 202 Information Security Standards, subchapter C Security Standards for Institutions of Higher Education (TAC 202). TAC 202 establishes a baseline of minimum Information Technology security controls and is subject to review every four years by the Texas Department of Information Resources (DIR). TAC 202 was revised effective February 2015 to more closely align with the Federal Information Security Management Act (FISMA), which references a more current and comprehensive catalog of information security controls based on the National Institute of Standard and Technology Special Publication 800-53 (NIST SP 800-53). Over the past three years, DIR has gradually implemented a Security Control Standards Catalog based on NIST standard SP 800-53 as a requirement for TAC 202 compliance. All controls in that catalog are now required effective February 2017. TAC 202 requires an audit at least every two years to ensure that all Texas institutions of higher learning, including UT Southwestern, are in compliance.

The Texas Department of Information Resources provides oversight and guidance to assist state agencies in developing policies and implementing information security programs that comply with the provisions of TAC 202. The UTSW Department of Information Security is responsible for implementing the institution's information security program. This department is led by the Associate Vice President and Chief Information Security Officer (CISO), who reports directly to the President. The System Access Management (SAM) group is responsible for UTSW network access management and reports to the Assistant Vice President for Systems and Operations.

## **Scope and Objectives**

The Office of Internal Audit has completed its TAC 202 Compliance audit. This is a required compliance audit and part of the fiscal year 2017 Audit Plan.

The scope covered the NIST control groups included in the TAC 202 control standards catalog, with a focus on three of the control groups: Access Control, Training and Awareness, and System and Information Integrity. Audit procedures included a risk assessment survey for the selected controls, conducting interviews, reviewing and evaluating supporting policies, procedures, and documentation to support the Medical Center's efforts to address and comply with TAC 202 requirements.

The primary objective of this audit was to evaluate the controls and processes in place to ensure compliance with Texas Administrative Code Chapter 202 Subchapter C (TAC 202) and assess the adequacy and effectiveness of policies and procedures.

## Executive Summary

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

### Conclusion

UT Southwestern generally complies with TAC 202, state and federal guidelines and UT System and UT Southwestern policies and procedures relative to information security. One opportunity for improvement was identified regarding notification of terminated and transferred users.


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

|              |          |            |         |           |
|--------------|----------|------------|---------|-----------|
| Priority (0) | High (0) | Medium (1) | Low (0) | Total (1) |
|--------------|----------|------------|---------|-----------|

Strengths identified during the audit include:

- Information Security has implemented real-time monitoring for unsuccessful user logon attempts for privileged administrator accounts.
- The FY17 Training Completion percentage for New Hire Training for the Information Security component is 100% as of July 24, 2017.
- The SAM group has increased the frequency of monitoring and disabling dormant network user accounts from a quarterly to a monthly basis.

One key improvement opportunity risk-ranked as medium is summarized below.

- 
**Ensure Department System Administrators Receive Notice of Terminated and Transferred Users** – Daily notice of terminated and transferred users is not distributed to administrators of all department systems where users can logon independent of their UTSW network access, which may result in excessive or unauthorized continued access if not removed timely.

Management has plans to address the issues identified in the report and in some cases have already implemented corrective actions. These responses, along with additional details for the key improvement opportunity listed above are listed 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.

## Executive Summary

---

Sincerely,

Valla F. Wilson, Associate Vice President for Internal Audit, Chief Audit Executive

**Audit Team:**

Gabriel Samuel, Senior IT Auditor

Jeffrey Kromer, Director, IT & Specialty Audit Services

cc: Kate Conklin, Associate Vice President for Institutional Compliance  
Arnim E. Dontes, Executive Vice President, Business Affairs  
John Malanowski, Associate Vice President, Human Resources  
Marc E. Milstein, Vice President, Information Resources and Chief Information Officer  
Daniel K. Podolsky, M.D., President  
David Reagan, Assistant Vice President, Systems & Operations  
Mary Robles, Manager, Information Resources  
Joshua Spencer, Associate Vice President and Chief Information Security Officer  
Ivan Thompson, Vice President and Chief Human Resources Officer

## Detailed Observations and Action Plans Matrix

|   |   |   |
|---|---|---|
| <p><b>Risk Rating: Medium</b> 🟡</p> <p><b>1. Ensure Department System Administrators Receive Notice of Terminated and Transferred Users</b></p> <p>Daily notice of terminated and transferred UTSW personnel distributed by the System Access Management (SAM) group does not include administrators of all department systems where users can logon independent of their UTSW network access, such as some cloud-based systems. As a result, there is a risk of excessive or unauthorized continued access for these terminated or transferred users if system administrators are not aware of the change in status for these users.</p> <p>Currently, daily notices are sent to a limited group of system administrators including Parkland Hospital, Children’s Health and administrators of eight other UTSW systems.</p> | <ol style="list-style-type: none"> <li>1. Identify all critical department systems where users can logon independent of their UTSW network access and, based on application owner familiarity with their user population, determine which application owners should receive notification of user terminations and transfers. To assist in identifying these systems, analyze the list of critical systems included in the Business Continuity Plan.</li> <li>2. Identify all applications included in Information System Acquisition Committee records where use of the central access system is not indicated and notify the respective application owners of the institution’s requirements for appropriate management of access.</li> <li>3. For systems not already included in Information System Acquisition Committee (ISAC) records, consider requiring identified application owners to attest to the appropriateness of their account management procedures.</li> </ol> | <p><b><u>Management Action Plans:</u></b></p> <ol style="list-style-type: none"> <li>1. Information Security has analyzed the full list of critical systems, and confirmed all non-administrative user-level access is either integrated into the central access management system or has other controls sufficient to ensure appropriate levels of risk regarding termination of access for terminated users, such as use of the daily termination reports.</li> <li>2. Information Security will notify all application owners who have registered their information systems via the Information System Acquisition form and have not indicated use of the central access system for their respective system. This notification will include requirements for appropriate management of access, utilization of the central access management system, and other resources should use of the centralized system not be feasible.</li> <li>3. All application owners identified in #2 will be required to acknowledge that their system utilizes appropriate account management procedures. This one-time process will address systems that predate current ISAC review procedures.</li> </ol> |
|---|---|---|

## Detailed Observations and Action Plans Matrix

|  |  |   |
|--|--|---|
|  | <p>4. Coordinate with the SAM group to add the identified application owners to the email distribution to ensure they receive timely notice to remove user access.</p> <p>5. As a long term solution for role-based security, move forward with plans to implement the Microsoft Identity Management (MIM) system.</p> | <p>4. If insufficient account management procedures identified in #2 exist, the department will be required to implement appropriate account management procedures which could include utilization of the central access system or daily notification of employee transfers and terminations.</p> <p><b><u>Action Plan Owners:</u></b></p> <p>Associate Vice President &amp; Chief Information Security Officer</p> <p><b><u>Target Completion Dates:</u></b></p> <p>1. Completed<br/>2. October 1, 2017,<br/>3,4. December 31, 2017</p> <p>5. As a long-term solution, Information Resources is implementing Microsoft Identity Management (MIM), which will provide the capability to more readily manage access in an automated and centralized manner to a variety of systems. The systems within the current project are Epic and PeopleSoft. Additional systems will be evaluated and integrated as appropriate upon completion of the initial project.</p> |
|--|--|---|

## Detailed Observations and Action Plans Matrix

|  |  |   |
|--|--|---|
|  |  | <p><b><u>Action Plan Owners:</u></b></p> <p>Associate Vice President, Human Resources</p> <p>Vice President, Information Resources and Chief Information Officer</p> <p>Associate Vice President and Chief Information Security Officer</p> <p><b><u>Target Completion Dates:</u></b></p> <p>Evaluation of integration of additional systems to begin June 1, 2018. Implementation will be ongoing.</p> |
|--|--|---|



## 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:

|   |  |  |
|---|--|--|
| <b>Risk Definition-</b> The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management. | <b>Degree of Risk and Priority of Action</b> |  |
|   | <b>Priority</b>                              | 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.   |
|   | <b>High</b>                                  | 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. |
|   | <b>Medium</b>                                | 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.              |
|   | <b>Low</b>                                   | 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.