Office of Internal Audit

UT Southwestern Medical Center

The University of Texas Southwestern Medical Center
TAC 202 Compliance

Internal Audit Report 15:31

October 8, 2015

UTSouthwestern Medical Center

Executive Summary

Background

Created in 1977 by the Texas Legislature, the Texas Administrative Code (TAC) is a compilation of all state agency rules in Texas. The portion of the code applicable to UTSW 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 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). Legacy TAC 202 was prescriptive with nine sections and a total of 151 risks. The revised February 2015 TAC 202 is less granular with six sections and 72 risks. Over the next two years, DIR will be gradually implementing a new controls catalog based on NIST SP 800-53 as a requirement for TAC 202 compliance. 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, with a staff of nine employees, is responsible for implementing the institution's information security program. This department is led by the Assistant Vice President and Chief Information Security Officer (CISO), who reports directly to the President.

Scope and Objectives

The audit covered the period of September 1, 2014 to August 30, 2015. This review is part of the Fiscal Year 2015 Internal Audit Plan. Audit procedures included 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. We performed activities to evaluate policy statements and processes in the following six new sections of TAC 202: Management Responsibilities, Staff Responsibilities, Security Reporting, Security Program, Managing Security Risks, and Security Standards.

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.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

UT Southwestern Medical Center

Executive Summary

Conclusion

The process, policies, and activities related to the information security program are well-established and address the current TAC 202 requirements. The Chief Information Security Officer has an in-depth understanding of the rules and regulations covered in TAC 202 and he is dedicated to ensuring UT Southwestern's compliance with DIR information security standards. While no exceptions were noted in five of the six policies and processes categories in TAC 202, policies and practices related to Security Reporting did not meet expectations.

Included in the table below is a summary of the observation noted, along with the respective disposition of this observation within the UTSW internal audit risk definition and classification process. See Appendix A for Risk Rating Classification and Definitions.

High (0)	Medium/High (0)	Medium (1)	Low (0)	Total (1)

There was one medium risk issue identified:

- **Update and test the Data Breach Incident Response plan. –** The current Data Breach Incident Response plan requires updating to clarify how and in what circumstances a joint-coordinated communication plan is warranted, and to consider any new requirements based on the UT Cyber Liability insurance policy.

The details of this observation, recommendations and management action plan can be found in the detailed section of the report below.

With the exception of the one Medium Risk observation above, this review of the current TAC202 security standards for FY2015 indicates a progressively robust development of Information Security controls at UT Southwestern.

Management has implemented or is in the process of implementing corrective action plans. Management responses are listed in the Detailed Observations and Action Plans Matrix section of this report.

We appreciate the professional courtesy and assistance received throughout the audit from the offices of Compliance, Communications, Marketing and Public Affairs, and the Chief Information Security Officer.

Executive Summary

Sincerely,

Valla F. Wilson, Assistant Vice President for Internal Audit

Audit Team:
John Maurer, Senior IT Auditor
Jeffrey Kromer, Director of IT and Specialty Audit Services
Valla Wilson, Assistant Vice President for Internal Audit

Cc: Daniel K. Podolsky, M.D., President
Arnim Dontes, Executive Vice President for Business Affairs
Kirk A. Kirksey, Vice President for Information Resources
Steve Moore, Vice President, Communications, Marketing and Public Affairs
Joshua Spencer, Assistant Vice President and Chief Information Security Officer
Sharon Parsley, Assistant Vice President, Compliance

UT Southwestern Medical Center

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium **1. Update and test the Data Breach Incident Response plan.** Information Security, Compliance, and CMPA have a documented plan for assessing, investigating, evaluating, and reporting significant breach events but, currently, it is outdated and being revised. The current plan is not clear how and in what circumstances a joint-coordinated communication plan is warranted. In addition, the UT System has recently procured a new Cyber Liability insurance policy but how the new insurance provisions may affect the relevant data breach processes is undefined, and may require contracting with a new credit bureau and/or identity protection provider.	1. Information Security, CMPA, and Compliance leadership should jointly revise the Data Breach Incident Response plan. This plan should consider any necessary cyber liability insurance requirements as well as coordination of communications. 2. Following revision of the Data Breach Incident Response plan, it should be tabletop tested with the participation of appropriate department and executive management.	**Management Action Plans:** 1. We agree and will revise the Data Breach Incident Response plan. 2. Following the revision, we will test the new plan with a significant data breach scenario in view. **Action Plan Owners:** Assistant Vice President and Chief Information Security Officer Vice President of Communications, Marketing and Public Affairs Assistant Vice President of Compliance **Target Completion Dates:** 1. Contingent upon finalization of scope and guidance by UT System on the new cyber liability coverage (to include required data breach protocols) by October 31, 2015 and assuming the coverage does not require new contracts to be signed by UTSW, completion by January 31, 2016. 2. Testing completed and results evaluated by March 31, 2016.

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:

	Degree of Risk and Priority of Action	
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.	**High**	The degree of risk is unacceptable and either does or could pose a significant level of exposure to the organization. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	Medium/High	The degree of risk is substantially undesirable and either does or could pose a moderate to significant level of exposure to the organization. As such, prompt action by management is essential in order to address the noted concern and reduce risks to the organization.
	Medium	The degree of risk is undesirable and either does or could pose a moderate level of exposure to the organization. As such, action is needed by management in order to address the noted concern and reduce risks to a more desirable level.
	Low	The degree of risk appears reasonable; however, opportunities exist to further reduce risks through improvement of existing policies, procedures, and/or operations. 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.