Office of Internal Audit
800 W. Campbell Rd. SPN 32, Richardson, TX 75080
Phone 972-883-4876 Fax 972-883-6846

December 3, 2015

Dr. Hobson Wildenthal, President *ad interim*
Ms. Lisa Choate, Chair of the Institutional Audit Committee:

We have completed an audit of Texas Administrative Code (TAC) 202 Security Controls Standards as part of our fiscal year 2015 Audit Plan, and the report is attached for your review. The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The objective of our audit was to provide assurance that UT Dallas is in compliance with TAC 202 Security Control Standards.

Overall, we found that UT Dallas Information Security policies comply with TAC 202 Security Control Standards. The attached report details recommendations that will provide enhanced clarity for policies and enforcement.

Management has reviewed the recommendations and has provided responses and anticipated implementation dates. Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation subsequent to the anticipated implementation dates. We appreciate the courtesies and considerations extended to us during our engagement. Please let me know if you have any questions or comments regarding this audit.

Toni Stephens
Institutional Chief Audit Executive

UT Dallas Responsible Parties:
Nate Howe, Chief Information Security Officer

Members of the UT Dallas Institutional Audit Committee:
External Members:
Mr. Bill Keffler
Mr. Ed Montgomery
Ms. Julie Knecht
Dr. Inga Musselman, Acting Provost
Dr. Calvin Jamison, Vice President for Administration
Mr. Terry Pankratz, Vice President for Budget and Finance
Mr. David Crain, Vice President and Chief Information Officer
Dr. Bruce Gnade, Vice President for Research
Dr. George Fair, Vice President for Diversity and Community Engagement; Compliance Officer
Dr. Gene Fitch, Vice President for Student Affairs
Mr. Timothy Shaw, University Attorney

The University of Texas System:
System Audit Office

State of Texas Agencies:
Legislative Budget Board
Governor's Office
State Auditor's Office
Sunset Advisory Commission

Executive Summary

TAC 202 Security Control Standards, Report No. 1605

Audit Objective and Scope: The objective of our audit was to provide assurance that UT Dallas is in compliance with TAC 202 Security Control Standards. Our scope covered fiscal year 2015 operations.

The following is a summary of the audit recommendations by risk level. See the Appendix for additional details.

Recommendation	Risk Level	Estimated Implementation Date
(1) Update Policies to Require 128-bit Encryption	**Low**	Implemented during audit
(2) Finalize the Security Incident Response Procedure	**Low**	Implemented during audit

Responsible Vice President: Terry Pankratz, Vice President for Budget and Finance	**Responsible Party:** Nate Howe, Chief Information Security Officer

Staff Assigned to Audit: Colby Taylor, IT Auditor

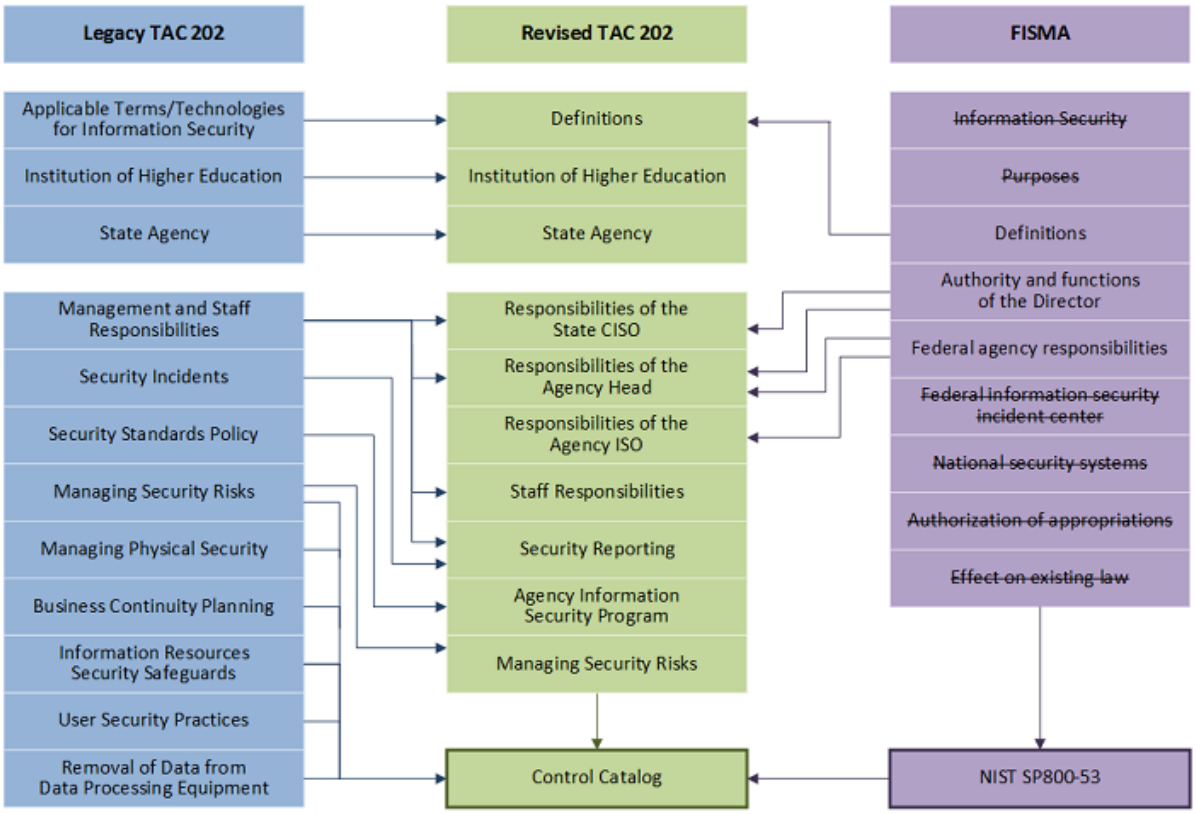
Table of Contents

Background

Texas Administrative Code (TAC) Title 1, Part 10, Chapter 202, *Information Security Standards, Subchapter C, Security Standards for Institutions of Higher Education*, outlines the security policies of the State of Texas that apply to all state institutions of higher education as follows:

Section	Description
§202.70	Responsibilities of the Institution Head
§202.71	Responsibilities of Information Security Officer
§202.72	Staff Responsibilities
§202.73	Security Reporting
§202.74	Institution Information Security Program
§202.75	Managing Security Risks
§202.76	Security Control Standards Catalog

As of February 2015, TAC 202 has been updated by a statewide committee of information security officers to move it closer to Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. The revised TAC covers agency responsibilities and includes a Control Standards Catalog.



Graphic showing TAC 202 changes and how they align to FISMA

Per the Texas Department of Information Resources (DIR), the Security Control Standards Catalog was "*initiated by DIR to help state agencies and higher education institutions implement security controls. It specifies the minimum information security requirements that state organizations must employ to provide the appropriate level of security relevant to level of risk.*"

The Chief Information Security Officer, reporting to the Vice President for Budget and Finance, has led the Information Security Office since 2014 and has been designated as the responsible party for ensuring compliance with TAC 202. Under the new leadership, the Information Security Office has demonstrated a commitment to TAC 202 compliance and best practices. The Information Security Office serves as a partner and educator. Risk mitigation is achieved through awareness training, technology solutions, inclusion of security controls in new projects, and regulatory compliance.

Audit Objective

The objective of our audit was to provide assurance that UT Dallas is in compliance with TAC 202 Security Control Standards.

Scope and Methodology

The scope of this audit was FY15 and our fieldwork concluded on November 19, 2015. To satisfy our objectives, we performed the following:

- Reviewed and gained an understanding of existing State, Federal, UT System, and UT Dallas policies and procedures over information security
- Tested supporting documentation and identified controls for compliance with TAC 202 Security Control Standards

Where applicable, we conducted our examination in accordance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance or audit work, and management of the internal auditing department.

Audit Results and Management's Responses

Controls
Our audit work indicated that the following controls currently exist:

- UT Dallas has a comprehensive Information Security and Acceptable Use policy.
- Information Security has a detailed contract analysis flowchart for data security risks.

- Thorough account management standards exist to provide guidance for all department applications.
- Published standards are in place for data storage and disposal.

Audit Recommendations

Priority Findings – UT System: A UT System priority finding is defined by the UT System Audit Office as: "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"[1] We have **no UT System Priority Findings** resulting from this audit.

However, although the above controls are in place, opportunities exist to make improvements to the existing TAC 202 guidance by implementing the recommendations outlined below.

(1) ***Update Policies to Require 128-bit Encryption***
Risk Rating: Low ★

From the Security Control Standards Catalog, Section SC-8, Implementation: *"Confidential information that is transmitted over a public network (e.g.: the Internet) must be encrypted with, at minimum a 128-bit encryption algorithm. An organization may also choose to implement encryption for other data classifications."*

Although UT Dallas is requiring encryption (and explicitly identifies programs that support desktop encryption that meet or exceed the minimum recommended level), the actual policies are not explicitly mandating a minimum of 128-bit encryption. Without a minimum level of encryption being specified, weak encryption could be utilized giving false assurance of data confidentiality/integrity.

Recommendation: Update policies to require a minimum of 128-bit encryption.

Management's Response: *Regarding the policy not explicitly mandating a minimum of 128-bit encryption (relates to SC-8), we agree with the spirit of the issue.*

- *We will not be putting specific key strength into the Information Security and Acceptable Use Policy, because this document is meant to deal with expectations and concepts, while not prescribing specific technical details (today's acceptable encryption strength may be considered tomorrow's weak encryption). The ISAUP does, however, empower us to set Standards, which we publish to the https://www.utdallas.edu/infosecurity/policy/ website after collecting feedback from stakeholders.*

[1] The appendix defines the risk levels for all internal audit recommendations.

- *All Standards currently on our website, https://www.utdallas.edu/infosecurity/policy/, will be updated to include 128-bit encryption as a minimum strength for data in transit over public networks. This specific encryption directive will not be applicable to data at rest. The following standards have been updated as a result of the Internal Audit recommendation, and our website administrator tells us they will be posted on 11/23/15.*

    - *Server Standard*
    - *Web-based Application Standard*
    - *Database Standard*

Estimated Date of Implementation: *Implemented during the course of the audit.*

Person Responsible for Implementation: *Nate Howe, Director of Information Resources, CISO*

(2) ***Finalize the Security Incident Response Procedure***
Risk Rating: Low ★

The Security Incident Response Procedures that guide the Information Security office when handling an incident are currently only a draft and were not finalized at the time of our audit.

In the Incident Analysis report provided, there is no indication of the severity level that the incident was classified as. Also, while the analysis does indicate who was communicated with during the incident, it does not indicate if the CISO, Dean or department head were notified at the end of the incident. Without finalized procedures, departmental staff may not be aware of the proper protocols, and appropriate personnel may not be properly notified when an incident occurs.

Recommendation: The Security Incident Response Procedures should be finalized, and consideration should be given to including the severity level and personnel to be notified.

Management's Response: *Regarding the incident response procedures (relates to SC-5), we agree with the spirit of the issue.*

- *We created a new template which includes severity levels that match the procedure, it is included as the appendix to the attached procedure*
- *We also added a Parties Notified area the template an area that helps ensure consistent reporting to external contacts.*
- *We formalized the Incident Response Procedures by removing the word Draft and updating the date.*

Estimated Date of Implementation: *Implemented during the course of the audit.*

Person Responsible for Implementation: *Nate Howe, Director of Information Resources, CISO*

Status of Prior Audit Recommendations

The following is the status of implementation of the recommendations resulting from Internal Audit Report No. R1326, *TAC 202*, dated August 5, 2013. Based on the progress and commitment to resolution by the new leadership in Information Security, most issues have been implemented.

Recommendation	Status	Estimated Date of Implementation
(1) **Significant** - Enhance Monitoring of Publicly Shared Confidential Information	Partially Implemented	August 31, 2017
(2) **Significant** - Encrypt Confidential Information in Transit	Implemented	
(3) **Significant** - Develop a Comprehensive Process for Patch Management	Implemented	
(4) Enhance Configuration Management	Implemented	
(5) Develop an Inventory of Information Resources	Implemented	
(6) Develop a Comprehensive, Effective Logging Strategy	Implemented	
(7) Improve Tools Used to Identify Confidential Information	Partially Implemented	August 31, 2017
(8) Controls over Data Storage Media Should Be Enhanced	Implemented	
(9) Prepare a Risk Assessment in Accordance with TAC 202 Requirements	Implemented	
(10) Enhance the Information Security Program	Implemented	
(11) Remediate Vulnerabilities in a Timely Manner	Implemented	
(12) The Information Security RAMP Should Be Improved	Implemented	

Conclusion

Based on the audit work performed, we conclude that the policies in place cover the current expected TAC 202 guidance and that there are only some minor tweaks that will provide better clarity in TAC 202 implementation.

We appreciate the courtesy and cooperation received from the management and staff in Information Security as part of this audit.

Appendix: Priority Findings and Risk Matrix

Definition of Risks

Risk Level	Definition
Priority	High probability of occurrence that would significantly impact UT System and/or UT Dallas. Reported to UT System Audit, Compliance, and Management Review Committee (ACMRC). Priority findings reported to the ACMRC are defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"
High	Risks are considered to be substantially undesirable and pose a moderate to significant level of exposure to UT Dallas operations. Without appropriate controls, the risk will happen on a consistent basis.
Medium	The risks are considered to be undesirable and could moderately expose UT Dallas. Without appropriate controls, the risk will occur some of the time.
Low	Low probability of various risk factors occurring. Even with no controls, the exposure to UT Dallas will be minimal.

Risk Factors

- Reputation - damage to the image of UT Dallas and/or UT System
- Information Security - integrity, confidentiality and availability of information
- Compliance – compliance with external legal or regulatory requirements
- Accomplishment of Management's Objectives – goals being met, projects being successful
- Effectiveness and Efficiency – objectives at risk and/or resources being wasted
- Capital Impact - loss or impairment of the use of assets
- Life Safety – including loss of life, injury, toxics/infectious disease
- Management Oversight – oversight duties performed by management
- Operational Alignment – management's alignment of people, process and technology to efficiently accomplish organization objectives
- Designed Controls – adequacy of controls within critical operations
- Payments/Expenditures – including fines and legal costs
- Lost Revenue – actual and/or opportunities