THE UNIVERSITY OF TEXAS AT DALLAS
OFFICE OF INTERNAL AUDIT
800 W. CAMPBELL RD. SPN 32, RICHARDSON, TX 75080
PHONE 972-883-4876 FAX 972-883-6846

June 27, 2018

Dr. Richard Benson, President,
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 2018 Audit Plan. The objective of our audit was to provide assurance that UT Dallas is in compliance with Texas Administrative Code (TAC) 202 Security Control Standards, specifically those relating to Incident Response and Configuration Management.

Overall, we found that UT Dallas generally complies with the TAC 202 Security Controls Catalog Standards relating to Incident Response and Configuration Management; however, the attached report details opportunities to improve compliance. 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, CPA, CIA, CRMA
Chief Audit Executive

Executive Summary

Audit Objective and Scope

The objective of our audit was to provide assurance that UT Dallas is in compliance with Texas Administrative Code (TAC) 202 Security Control Standards, specifically those relating to Incident Response and Configuration Management. The scope of this audit was fiscal year 2016 to date.

Conclusion

Overall, we found that UT Dallas generally complies with the TAC 202 Security Controls Catalog Standards relating to Incident Response and Configuration Management; however, the attached report details opportunities to improve compliance.

Audit Recommendations by Risk Level

Recommendation	Risk Level	Estimated Implementation Date
(1) Fully Implement the Incident Response Plan	High	(a) August 31, 2018 (b) December 31, 2018 (c) December 31, 2018
(2) Standardize Configuration Management	High	December 15, 2018
(3) Develop More Specific Procedures to Assist OIT and Distributed IT Organizations in Responding to Incidents	Medium	December 31, 2018
(4) Streamline Change Management Policy with Cherwell	Low	August 31, 2018
(5) Consistently Report Information to the Texas Department of Information Resources	Low	Implemented
(6) Improve Incident Response Plan Compliance with UTS 165 and TAC 202	Low	December 31, 2018

Responsible Vice Presidents

- Terry Pankratz, VP for Budget and Finance (Recommendations 1, 3, 5, 6)
- Frank Feagans, Vice President and Chief Information Officer (Recommendations 2, 4)

Responsible Parties

- Nate Howe, Chief Information Security Officer (Recommendations 1, 3, 5, 6)
- Brian Dourty, AVP and CTO, Office of Information Technology (Recommendations 2, 4)
- Debra Greszler, Manager Information Resources (Recommendation 4)

Staff Assigned to Audit

Project Manager: Toni Stephens, CPA, CIA, CRMA
Staff: Chris Robinette, IT Staff Auditor; Student Interns: Jan McDonald, Shivika Panjrattan

Report Distribution

Members of the UT Dallas Institutional Audit Committee
External Members
- Ms. Lisa Choate, Chair
- Mr. Gurshaman Baweja
- Mr. Bill Keffler
- Mr. Ed Montgomery
- Ms. Julie Knecht

UT Dallas Members
- Dr. Richard Benson, President
- Dr. Hobson Wildenthal, Executive Vice President
- Dr. Kyle Edgington, Vice President for Development and Alumni Relations
- Mr. Frank Feagans, Vice President and Chief Information Officer
- Dr. Gene Fitch, Vice President for Student Affairs
- Dr. Calvin Jamison, Vice President for Administration
- Dr. Inga Musselman, Provost and Vice President for Academic Affairs
- Dr. Joseph Pancrazio, Vice President for Research
- Mr. Terry Pankratz, Vice President for Budget and Finance
- Mr. Timothy Shaw, University Attorney, ex-officio

Responsible Parties
- Nate Howe, Chief Information Security Officer (Recommendations 1, 3, 5, 6)
- Brian Dourty, AVP and CTO, Office of Information Technology (Recommendations 2, 4)
- Debra Greszler, Manager Information Resources (Recommendation 4)

External Agencies
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

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

Per the Texas Department of Information Resources (DIR), the Security Control Standards Catalog[1] 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.*"

UTS 165 – Information Resources Use and Security Policy establishes expectations and guidelines from the University of Texas System on use of Information Technology within the institutions.

Per Section 2 of UTS 165: *"Information Resources residing in the Institutions of the University of Texas System are strategic and vital assets belonging to the people of Texas. Access to these resources shall be appropriately managed. It is the policy of The University of Texas System to protect Information Resources based on Risk against accidental or unauthorized access, disclosure, modification, or destruction and assure the availability, confidentiality, and integrity of these resources while avoiding creation of unjustified obstacles to conducting business and achieving the missions of the U. T. System."*

The Chief Information Security Officer, reporting to the Vice President for Budget and Finance, leads the Information Security Office (ISO) and is designated as the responsible party for compliance with TAC 202 & UTS 165. The Information Security Office serves as a partner and educator, and demonstrates a commitment to TAC 202 compliance and best practices. Risk mitigation is achieved through awareness training, technology solutions, inclusion of security controls in new projects, and regulatory compliance.

[1] http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf

Audit Objective

The objective of our audit was to provide assurance that UT Dallas is in compliance with Texas Administrative Code (TAC) 202 Security Control Standards; specifically those relating to Incident Response and Configuration Management.

Scope and Methodology

The scope of this audit was FY 16 to date, and our fieldwork concluded on June 1, 2018. To satisfy our objectives, we performed the following:

- Conducted a risk assessment specific to UT Dallas of the controls listed in the Security Controls Standards. Based on the risk assessment, we decided to focus on the incident response plan and configuration management.
- Reviewed and gained an understanding of existing UT Dallas policies and procedures over incident response planning and configuration management.
- Determined compliance with TAC 202 Security Controls Catalog Standards over incident response planning and configuration management by performing tests, observations, and interviews with responsible parties.

We conducted our examination in conformance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* are statements of core requirements for the professional practice of internal auditing.

Additionally, we conducted the audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results and Management's Responses

Strengths and Controls Noted During the Audit
The Incident Response Plan shared by ISO articulates the roles of individual teams and departments in the responding to security incidents at a high level.
The security standards produced by ISO are readily available on the UT Dallas website for reference by both end-users and UTD Information Technology (IT) entities.
ISO maintains a well-organized area for isolating infected devices and conducting digital forensics.

Strengths and Controls Noted During the Audit
The Annual Report produced by ISO provides comprehensive information on ongoing security efforts at UT Dallas and the risks that face the institution.
The Office of Information Technology (OIT) maintains a Change Management policy that standardizes the processing of changes within OIT's environment.
OIT conducts a weekly Change Management conference call to discuss upcoming changes and impacts of the previous changes. OIT includes other important entities such as ISO to encourage collaboration.
Change notifications are communicated well and in advance to the stakeholders by OIT. Additionally, the change calendar is visible to all the employees increasing visibility of the change to potential stakeholders.

Although the above strengths and controls were noted, other opportunities to strengthen the policies and procedures around TAC-202 and UTS 165 compliance are listed below. Risk levels are defined in the Appendix.

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
(1) ***Fully Implement the Incident Response Plan*** (High Risk) We tested the Incident Response Plan and noted the following: • The Incident Response Plan has not been incorporated into contingency planning within ISO or other departments. • OIT and departmental IT organizations have not been trained on the incident response plan or expected actions. ISO has discussed the plan as a department. • The plan has not been formally tested with ISO and other IT organizations. Most	Without a fully implemented incident response plan, there may be gaps in UT Dallas' ability to quickly and effectively respond to security incidents in a consistent, organized manner.	(a) Continue efforts with SecureWorks to coordinate testing internally and with other IT groups within UTD. (b) Opportunities should be identified to train other departments on the plan and ensure a public facing component of the plan should be developed for distribution on the Information Security webpage. (c) The Plan should be incorporated into Business Continuity Planning.	**Management's Response and Action Plans:** (a) ISO has contracted with SecureWorks to coordinate an onsite incident training event. A report and attendance list will be available after the event. (b) ISO incident response documentation will be added to Confluence to facilitate sharing within the organization. Limited details such as contact information and incident definitions will be shared on the Internet using the

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
testing is done by reviewing policies after they are used operationally. ISO is planning to coordinate with SecureWorks to conduct a formal test of the plan. • The plan has not been disseminated to other departments that would have involvement in incident response.			Frequently Asked Question format. (c) ISO agrees that recovery from an incident will be more effective if disaster recovery steps are documented within business continuity plans. Though ISO is not assigned responsibility for developing or testing business continuity and disaster recovery plans across the enterprise, the ISO will conduct a meeting with the EHS department for the purpose of conveying our shared concern that incident response plans for IT systems be incorporated into schools and department recovery plans. **Estimated Dates of Implementation:** (a) August 31, 2018 (b) December 31, 2018 (c) December 31, 2018 **Person Responsible for Implementation:** Nate Howe, CISO
(2) ***Standardize Configuration Management*** (High Risk)	Without a standard policy for all entities within OIT, configuration changes may not be consistently managed for each	OIT should develop a policy that addresses configuration management for each	**Management's Response and Action Plan:** OIT will review current configuration

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
Processes for controlling configuration changes are managed individually by application teams, and no OIT-wide policy exists. TAC 202's Configuration Management section requires that the organization establish a process for controlling modifications to hardware. A policy for configuration management should address the following areas: • Approval Process • Segregation of Duties • Responsibilities of involved teams/individuals • Process for coordinating across multiple teams • Commitment from management • Communication with users • Documentation requirements for each configuration change	application, increasing the opportunity for disruptions.	application managed by OIT.	management practices across the division and use this as input for developing a division wide configuration management process. **Estimated Date of Implementation:** December 15, 2018 **Person Responsible for Implementation:** Brian Dourty, AVP and CTO, Office of Information Technology
(3) ***Develop More Specific Procedures to Assist OIT and Distributed IT Organizations in Responding to Incidents*** (Medium Risk) While the incident response plan is no longer in the draft phase, it currently provides guidance at a high level. Currently, the plan does not have a significant number of detailed procedures for OIT and decentralized IT	Without specific details on procedures to take in response to suspected security incidents, responses to incidents may be inconsistent.	ISO should develop the Incident Response Plan to have more detail on responses to types of incidents that can be referenced by local IT organizations.	**Management's Response and Action Plan:** ISO agrees that additional detail should be documented in support of the Incident Response Plan. The additional detail will be published to Confluence and will include at least three new appendices to the plan. **Estimated Date of Implementation:** December 31, 2018

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
departments to reference in the event of an incident. The Information Security Office is working to develop more procedures (such as malware response) that can assist departmental IT support functions in effectively responding to incidents, though this is still a new effort for the team.			**Person Responsible for Implementation:** Nate Howe, CISO
(4) ***Streamline Change Management Policy with Cherwell*** (Low Risk) TAC-202, Control CM-4 states: *"The organization analyzes changes to the information system to determine potential security impacts prior to change implementation."* UTS 165, Standard 7 requires *"assessment of potential impacts of changes, including the impact on Data classification, Risk assessment, and other security requirements."* We tested change management controls and noted the following: • The ISO participates in the change management calls and then reviews the changes; however, there is no documentation of the security implications of the change in the change management	Without consistent documentation of security impacts in Cherwell, changes may be implemented without fully addressing the security implications.	OIT should streamline the change management policy within the Cherwell application by improving documentation on security impacts, incorporate risk scoring based on security and data classification into the Risk Level Assessment matrix, require documentation of approval within Cherwell for emergency changes, and require go/no-go documentation for changes that reach a certain risk threshold.	**Management's Response and Action Plan:** (a) OIT will review the Change Management Process to ensure that any potential security impacts are identified in the Risk Level Assessment section of the Cherwell ticket. (b) Procedure will be updated to require Emergency Changes have approval documented in Cherwell tickets. (c) OIT will require that the Acceptance Criteria section in Cherwell include the criteria for a go (validation criteria) and what would constitute a no -go (back out) of the change. **Estimated Date of Implementation:** August 31, 2018 **Person Responsible for Implementation:**

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
tool, Cherwell. • Per OIT Change Management policy, change owners must establish go/no-go criteria within the "Acceptance Criteria" field. Acceptance criteria are designated requirements for a change to be considered "implemented." Testing of changes from January 14 – 27, 2018 did not have go/no-go criteria clearly articulated. Acceptance criteria was outlined in most changes. • The two emergency changes we reviewed were conducted according to policy; however, the approval process was not immediately discernable from reviewing the changes within Cherwell. • OIT maintains a detailed matrix for rating proposed changes and estimating the impact upon the environment. These ratings do not include security or impact based on the classification of data on impacted systems, meaning that the full risk of a proposed change may not be considered.			• Debra Greszler, Manager, Information Resources • Brian Dourty, AVP and CTO

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
(5) ***Consistently Report Information to the Texas Department of Information Resources*** (Low Risk) ISO does adhere to reporting for specific incidents that meet a certain criteria to both UT System and the Department of Information Resources. TAC 202, Control IR-6 requires monthly reports: *"Summary reports of security -related events shall be sent to the department on a monthly basis no later than nine (9) calendar days after the end of the month. Organizations shall submit summary security incident reports in the form and manner specified by the department. Supporting vendors or other third parties that report security incident information to a state organization shall submit such reports to the state organization in the form and manner specified by the department, unless otherwise directed by the state organization."* In the past several months, summarizations of incidents have not been sent to the Department of Information Resources due to an internal communications error. Per TAC 202, organizations a required to provide monthly summaries	Inconsistent reporting to the Department of Information Resources may put UT Dallas in noncompliance with TAC 202 requirements and will inhibit the Texas DIR's ability to determine trends in incidents.	ISO should consistently provide reports required by TAC 202 to the Texas DIR.	**Management's Response and Action Plan:** ISO has implemented additional reporting to DIR. An example of the most recent reporting upload is attached (*given to Internal Audit but not included in the audit report*). We consider this closed during the audit period and intend to continue the process monthly. **Estimated Date of Implementation:** Implemented at the time of audit. **Person Responsible for Implementation:** Nate Howe, CISO

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
to the Texas Department of Information Resources (DIR).			
(6) ***Improve Incident Response Plan Compliance with UTS 165 and TAC 202*** (Low Risk) The following opportunities exist to improve compliance with UTS 165 and TAC 202: • The plan was last updated in March 2018, and the plan does reference the requirement for updates; however, the frequency of these updates is not specifically defined. • The Incident Response Plan does not have the following specific criteria required by UTS 165: o Guidelines for addressing potential damage of security incidents o Guidance on preserving physical and electronic evidence o Specific methods of communication that will be used when coordinating with affected users or outside organizations	Without addressing the specific criteria outlined by UTS 165 and TAC 202, response to incidents may not be effective.	Implement procedures to address all incident response plan requirements outlined in UTS165 and TAC 202. Ensure that the procedures are linked within the Incident Response Plan.	**Management's Response and Action Plan:** ISO intends to update the Incident Response Plan annually and will include the recommended improvements in the next revision, to promote harmony with TAC 202 and UTS-165. **Estimated Date of Implementation:** December 31, 2018 **Person Responsible for Implementation:** Nate Howe, CISO

Conclusion

Overall, we found that UT Dallas generally complies with the TAC 202 Security Controls Catalog Standards relating to Incident Response and Configuration Management. Implementation of the recommendations will enhance compliance and the effectiveness of Incident Response and Configuration Management.

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

Appendix

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 Risk Management Committee (ACRMC). Priority findings reported to the ACRMC 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.