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

October 31, 2018

Dr. Richard Benson, President,
Ms. Lisa Choate, Chair of the Institutional Audit Committee:

We have completed an audit of the Education Research Center (ERC), as part of our fiscal year 2018 Audit Plan. The objective of our audit was to certify that the ERC at UT Dallas is in full compliance with all terms of the contract between the THECB and UT Dallas and all applicable state and federal laws. The report is attached for your review.

Overall, the ERC complies with the contract; however, the audit resulted in opportunities to improve compliance as well as strengthen information security controls. 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

To certify that the Education Research Center at UT Dallas is in full compliance with all terms of the contract between the THECB and UT Dallas and all applicable state and federal laws.

Conclusion

Overall, the Education Research Center complies with the terms of the contract between the THECB and UT Dallas. Implementation of the recommendations will help strengthen information security controls and compliance with the contract.

Audit Recommendations by Risk Level

Recommendation	Risk Level	Estimated Implementation Date
(1) *Ensure Patching Is Being Performed*	**Medium**	December 31, 2018
(2) *Establish More Effective Logging Capabilities*	**Medium**	October 31, 2018
(3) *Ensure IRB Proposals Are Updated for Research Projects*	**Medium**	September 30, 2018
(4) *Update Procedures for FERPA Review*	**Medium**	September 30, 2018
(5) *Update Terms and Conditions to Ensure Compliance with the THECB*	**Low**	Remediated during the audit
(6) *Ensure Keys Are Returned When Employees Terminate or Transfer*	**Low**	Remediated during the audit

Responsible Vice President

Dr. Joseph Pancrazio, Vice President for Research

Responsible Parties

- Rafael Martin, Associate Vice President for Research
- Greg Branch, Director for Texas Schools Project

Staff Assigned to Audit

Project Leader: Toni Stephens, CPA, CIA, CRMA, Chief Audit Executive
Staff: Chris Robinette, IT Staff Auditor

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
- Mr. Rafael Martin, Associate Vice President for Research
- Mr. Greg Branch, Director for Texas Schools Project

External Agencies
- The University of Texas System Audit Office
- Legislative Budget Board
- Governor's Office
- State Auditor's Office
- Sunset Advisory Commission
- Texas Higher Education Coordinating Board

UT Dallas Informational Copy
- Mr. Nate Howe, Chief Information Security Officer
- Ms. Sanaz Okhovat, Assistant Vice President, Office of Research Compliance

Table of Contents

Background

In 2006, the 79th Texas Legislature authorized the Commissioner of Education and the Texas Higher Education Coordinating Board (THECB) to establish statewide centers for education research. The Education Research Center (ERC)[1] at UT Dallas is charged with facilitating education research that will benefit Texas students from pre-kindergarten to college and into the workforce by providing approved researchers access to individual-level administrative data that can be used to study the progress and performance of students, teachers and schools. Currently, the ERC is handling 10 grant-funded projects (as tracked by Post Award Management), five of which are federally funded. The ERC began reporting to the Vice President for Research on September 1, 2018.

A contract was signed on September 1, 2017, to continue the authorization of an ERC at UT Dallas through August 31, 2024, unless extended. The contract states, "*At a minimum, the Internal Auditor of UTD shall annually certify that the ERC is in full compliance with all terms of this contract and all applicable state and federal laws."* The contract also stipulates that the ERC will report compliance with Information Security policies to the Chief Information Security Officer and the Assistant Vice President of Research Compliance annually. The primary requirements of the contract include responsibility of data and security of the confidential research data.

Audit Objective

To certify that the Education Research Center at UT Dallas is in full compliance with all terms of the contract between the THECB and UT Dallas and all applicable state and federal laws.

Scope and Methodology

The scope of this audit was the contract signed by the Education Research Center (ERC) and the Texas Higher Education Coordinating Board (THECB). Our fieldwork concluded on June 29, 2018. To satisfy our objectives, we performed the following:

- Reviewed the contract signed between the ERC and the THECB to gain an understanding of the requirements that the TSP is required to maintain.
- Reviewed TAC 202 regulations and the associated Security Controls Catalog.
- Conducted interviews with the Director of the ERC to determine the practices and controls that are in place to maintain confidential data.
- Reviewed financial payments to the THECB to ensure compliance.

[1] https://www.utdallas.edu/research/tsp-erc/utd-erc.html

- Determined if the TSP was properly securing data according to TAC 202 and THECB requirements.

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 ERC maintains a segmented network with strict controls in place to protect confidential data from leaving the network unless the data undergoes the FERPA review process and is cleared for public release.
Before access to confidential data is granted, principal investigators are required to sign confidentiality agreements and are given training by the Director of the ERC on the FERPA review expectations and process.
Data for projects is maintained in specific project folders that only can be accessed by authorized employees.
External media is disabled for all end-users and ERC computers, while the folders that house data are only accessible by personnel assigned to those projects. There are no installed printers on the ERC system, preventing end-users from printing data.
Administrative accounts are used solely for administrative functions; no project work is done using system admin or root access.
Hard drives no longer in use are wiped using DBAN software. Non-functioning PCs are stored behind the secured area.

Although the above strengths and controls were noted, other opportunities to strengthen information security controls and compliance with the contract are listed below. Risk levels are defined in the Appendix.

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
(1) ***Ensure Patching Is Being Performed*** *(*Medium Risk) During our review of the ERC system, the following items were noted: • The vendor no longer supports the NetApp server that houses data, and security patches are no longer released. • The compute server is not regularly patched. • The switches in the current setup have not received operating system updates since purchase in 2010. • The ASA router was last updated in 2014-2015. • ERC PCs have not received regular patching. According to Texas Administration Code (TAC) 202 Security Controls Catalog MA-6: *"The lack of processes for system maintenance may result in compromise of system security due to latest updates not being made to systems in a timely manner."*	Without routine patching, crucial security holes can be left open, which leaves the servers housing data open to known-exploits. This is highly mitigated by the relative inaccessibility of the servers from the rest of the network. Network equipment could have known vulnerabilities that are unpatched.	With the implementation of the new system, the ERC should ensure that vulnerability patching is fully supported with access to the university update repositories. Networking equipment should be updated to the most recent code levels for the ASA router and switches.	**Management's Response and Action Plan:** *Overall, an understanding has been reached with OIT for them to assume responsibility for the update and system maintenance of all server and networking components supporting the ERC. We are in the process of concluding an MOU (which was waiting for final rates and service-center approval), but have been proceeding under an agreement to move forward as though it were in place (which is how the UT Austin and U of H ERC's address central IT support).* *This was due to a number of aging system components that had been awaiting replacement during our (much-delayed) wholesale systems upgrade initiative. During this period, some of the legacy components fell out of support, or became impractical to maintain for technical reasons. The most critical of these have now been replaced entirely, and the remainder the peripheral components will be replaced as we proceed. During the period in question, all equipment with overdue updates was operating behind a*

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
			hard security perimeter on a sequestered network with stringent physical access controls. There has been no suggestion that the security of the ERC data (or any other confidential materials) was compromised. **Estimated Date of Implementation:** *See below for item specific status. Target for completion of all aspects of system cutover is December 31 for all ERC-supporting components.* **Person Responsible for Implementation:** *Gregory Branch, Director for the Texas Schools Project* ***Responses to Specific Findings:*** - Netapp: *The (now unsupported) Netapp storage device has been retired from service supporting the ERC program work. It still serves ancillary functions, and will be retired completely when the system upgrades have been completed. Storage for ERC projects is now provided by the new server that has been implemented.* - Compute Server: *Likewise, the (also unsupported) Cray blade server that was*

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
			serving as our compute server has also been retired from use in the ERC program, and replaced in its function by a new server under the management of OIT. - Internal Switches: *Current management was previously unaware of the necessity of support for this equipment. Our understanding with OIT is that these will be remediated before October 31, 2018.* - ASA/Router: *The ASA was determined to be sufficiently close to end-of-life for vendor support that continued update was not a viable approach to remediation. The ASA has now been replaced with newer model which is within support and up to date by OIT.* - *Internal Network PC's* These PC's within the secure network for the ERC program facility will be replaced by managed thin client machines imminently as part of the general upgrade project. At this time, they are in fact functioning only as thin clients, and do not directly access the secure data in the

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
			course of project work (rather they run terminal sessions on the new compute server). With the move to SCCM updating by the University, the updating procedure previously used for these machines became defunct and not easily remediable without allowing University central management tools access in through the ERC firewall, which would be present an unacceptable security vulnerability. Remediation will therefore occur with the replacement of our client access equipment no later than December 31, 2018.
(2) ***Establish More Effective Logging Capabilities*** (Medium Risk) According to the THECB contract, "*UTD ERC shall monitor access to and provide copies of logs to the THECB of researchers attempting to access and accessing the ERC data housed at UTD.*" System events are currently captured in Event Viewer on the respective Windows servers/PCs. Logging for the firewall is currently done through the ASA software, where it is stored in a raw text file on the PC.	With data in a raw format, it is difficult to identify any suspicious trends in user activity or network traffic.	As the new system is implemented, the ERC should ensure that effective logging is established and logs are routinely monitored.	**Management's Response and Action Plan:** *The current approach to logging access to the secure system is being replaced by the implementation of more appropriate and simplified logging facilities on the new ERC server.* **Estimated Date of Implementation:** *October 31, 2018* **Person Responsible for Implementation:** *Gregory Branch, Director for the Texas Schools Project*

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
(3) ***Ensure Institutional Review Board (IRB) Approvals Are Updated for Research Projects*** (Medium Risk) The THECB contract states that "*The UTD ERC shall provide evidence of approval from the IRB or justification for exclusion from the IRB process before a researcher has access to any data.*" During a review of IRB approvals for four projects, one was found to be out of date for IRB approval.	A lapse would result in a researcher without current IRB approval still maintaining access to the ERC data.	The ERC should institute a process to routinely review IRB approvals to ensure PIs who have a lapse do not maintain access to TSP data.	**Management's Response and Action Plan:** *The minimal review exempt determination letter identified as out of date during the audit was updated immediately and is current. Going forward, a review will be performed quarterly to ensure that IRB approvals/exempt determinations are kept current, and action taken to seek extensions for any that are approaching expiration.* **Estimated Date of Implementation:** *September 30, 2018* **Person Responsible for Implementation:** *Gregory Branch, Director for the Texas Schools Project*
(4) ***Update Procedures for FERPA Review*** (Medium Risk) Documentation for the Family Educational Rights and Privacy Act (FERPA) review process and access controls have not been updated since 2011. The current policy does not cover specific steps to take in the event of a FERPA violation.	As the team grows and a new system is implemented, a lack of consistent, updated documentation could result in inconsistent application of the controls for protecting the data. In addition, the University Registrar may not be properly notified if FERPA is violated.	The ERC should review existing procedures on access controls and the FERPA review process and ensure that it is updated with current practices. The ERC should also discuss current practices with the University Registrar, responsible for FERPA at UT Dallas, to ensure that all UTD responsible parties are included for FERPA violations.	**Management's Response and Action Plan:** *The written procedure for FERPA review is being revised to reflect more recent adjustments to our process, and the University Registrar will be consulted to inform this revision. To be clear, however, the information to which the release review process pertains does not involve UTD data, but rather statewide data obtained from State agencies under the ERC program for use in research.*

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
			Estimated Date of Implementation: *September 30, 2018.* **Person Responsible for Implementation:** *Gregory Branch, Director for the Texas Schools Project*
(5) ***Update Terms and Conditions to Ensure Compliance with THECB*** (Low Risk) The THECB contract states the following in regards to external media access: "*UTD ERC personnel will not store or transmit data on a portable storage device, such as, but not limited to, a USB flash drive, cellphone, portable laptop, external hard drive or through unencrypted e-mail, with the exception of system backup tapes located at a secure off-site location.*" Researchers are required to sign confidentiality agreements, which reference the Terms and Conditions, for access to data, and these agreements stipulate that data should not be removed from the system; however, they do not specifically outline the restrictions on external media access.	Not including THECB contract requirements in subcontracts may result in unauthorized access to confidential information and noncompliance with the THECB contract.	The ERC should ensure the Terms and Agreements comply with all terms of the THECB contract. Agreements with researchers should be adjusted to include explicit verbiage prohibiting the use of external media.	**Management's Response and Action Plan:** *An appropriately adapted version of the suggested language has been added to the terms and conditions document (referenced by confidentiality agreements signed by all users of the ERC and other instruments), and is now present in the operative version of this document going forward.* **Estimated Date of Implementation:** *Remediated* **(verified by Internal Audit)** **Person Responsible for Implementation:** *Gregory Branch, Director for the Texas Schools Project*

Observation and Risk Level	Risk/Effect	Recommendation	Management's Response and Action Plan
(6) Ensure Keys Are Returned When Employees Terminate or Transfer (Low Risk) Two keys to the server room had been signed out to previous directors but never returned upon their termination of employment with the University.	Unauthorized personnel may access the server room.	The ERC should emphasize procedures to ensure keys are returned when employees terminate employment or transfer to another department. Consideration should be given to having the server room rekeyed as a precautionary measure.	**Management's Response and Action Plan:** *The locks associated with the keys identified as missing were re-keyed (with evidence provided to Internal Audit). In general, physical key distribution is limited to the director and office manager/ASO, with the exception of the server room deadbolt lock, the key for which is also held by the research support/data manager. Access for all other personnel and affiliates is solely by card reader. Staff responsibilities relative to checkout have been clarified and appropriate staff have been directed to ensure that complete checkout protocol is observed for all departing employees, to include directors.* **Estimated Date of Implementation:** *Remediated* **(verified by Internal Audit)** **Person Responsible for Implementation:** *Gregory Branch, Director for the Texas Schools Project*

Conclusion

Overall, the ERC complies with the terms of the contract. Implementation of the recommendations in the report with help strengthen information security controls and compliance with the contract. We appreciate the courtesy and cooperation received from the management and staff in the Education Research Center 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 (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.