



April 16, 2015

Dr. Kirk A. Calhoun, M.D.  
UT Health Northeast  
11937 U. S. Hwy 271  
Tyler, TX 75708

Dr. Calhoun:

We have completed an engagement to determine the status of recommendations made by an external consulting firm concerning the institution's information technology (IT) vulnerabilities. The services were performed during FY 2013 at the request of Executive Management and the associated report was dated October 31, 2013. Executive Management requested for Internal Audit to subsequently include project hours in the FY 2015 Audit Plan to follow-up to determine and report the institution's progress in resolving the IT vulnerabilities identified by the consulting firm.

We focused our work on critical and higher risk IT vulnerabilities identified by the consulting firm. Overall, we found that Information Technology and Information Security are actively and collaboratively working together to reduce the institution's information technology vulnerabilities noted in the FY 2013 report as well as new critical vulnerabilities identified. Notable progress has been made in resolving a large number of the most critical vulnerabilities while progress on resolving some of the higher risk vulnerabilities is moving at a slower pace due to limited staffing, tools, or competing priorities. Per Texas Government Code §552.139, information about computer vulnerabilities is not subject to public disclosure. This report includes audit results that are sensitive in nature and detailed results, although provided to key members of internal management and Internal Audit Committee Members, will not be included in versions submitted outside the institution.

This audit was conducted in accordance with guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. We appreciate the assistance provided by management and other personnel and hope the information presented in our report is helpful.

Sincerely,

A handwritten signature in black ink that reads "Kris I. Kavasch".

Kris I. Kavasch  
Chief Audit Executive

Enclosure

cc:

Dr. Raymond S. Greenberg, UT System Executive Vice Chancellor for Health Affairs [rgreenberg@utsystem.edu](mailto:rgreenberg@utsystem.edu)

Mr. J. Michael Peppers, UT System Chief Audit Executive [systemauditoffice@utsystem.edu](mailto:systemauditoffice@utsystem.edu)

Mr. Richard St. Onge, UT System Associate Vice Chancellor for Shared Services [richardstonge@utsystem.edu](mailto:richardstonge@utsystem.edu)

Ms. Dyan Hudson, UT System Assistant Director, Specialty Audit Services [dhudson@utsystem.edu](mailto:dhudson@utsystem.edu)

Mr. Joe Woelkers, Executive Vice President, Chief Operating Officer [joe.woelkers@uthct.edu](mailto:joe.woelkers@uthct.edu)

Mr. John Yoder, Vice President, Information Technology, Chief Information Officer [john.yoder@uthct.edu](mailto:john.yoder@uthct.edu)

Ms. Donna Martin, Executive Director for Compliance and Information Security Officer [donna.martin@uthct.edu](mailto:donna.martin@uthct.edu)

Legislative Budget Board - [ed.osner@lbb.state.tx.us](mailto:ed.osner@lbb.state.tx.us)

Governor - [internalaudits@governor.state.tx.us](mailto:internalaudits@governor.state.tx.us)

State Auditor's Office - [iacoordinator@sao.state.tx.us](mailto:iacoordinator@sao.state.tx.us)

Sunset Advisory Commission - [sunset@sunset.state.tx.us](mailto:sunset@sunset.state.tx.us)



**Information Technology Security  
Assessment Follow-up Audit**

**April 16, 2015**

**UT HEALTH NORTHEAST  
OFFICE OF INTERNAL AUDIT  
11937 US HIGHWAY 271  
TYLER, TX 75708**

**UT Health Northeast  
IT Security Assessment Follow-up Audit  
Fiscal Year 2015**

---

**TABLE OF CONTENTS**

*Background*..... 4

*Audit Objective*..... 4

*Audit Scope and Methodology* ..... 4

*Audit Results* ..... 5

*Conclusion* ..... 5

*Summary of Priority Findings* ..... 6

**UT Health Northeast**  
**IT Security Assessment Follow-up Audit**  
**Fiscal Year 2015**

---

**Audit Report**

*Per Texas Government Code<sup>1</sup>, information about computer vulnerabilities is not subject to public disclosure. This report includes audit results that are sensitive in nature and detailed results will not be included in versions submitted outside the institution.*

***Background***

This engagement was completed as part of our FY 2015 Audit Plan in the area of Information Technology Audits. During FY 2013, UT Health Northeast senior leaders identified a need to determine the status of the institution's information security and the level of risk it was incurring. As a result, the institution hired an external consulting firm to perform an assessment of its information security strategy and resulting vulnerabilities. To monitor the progress made in resolving the institution's known IT vulnerabilities, senior leaders requested for Internal Audit to include project hours in their FY 2015 Audit Plan for following up and reporting the status of recommendations made by the consultants for resolving UT Health Northeast's IT vulnerabilities.

***Audit Objective***

The objective of this audit was to assess the implementation status of the recommendations that address the institution's higher risk IT vulnerabilities as outlined in the FY 2013 externally contracted IT Security Assessment and the associated report dated October 31, 2013.

***Audit Scope and Methodology***

The scope of our audit was FY 2015 (through the report date). To achieve the objective we completed the following:

- Interviewed Information Technology and Information Security management and relevant staff
- Reviewed applicable policies and procedures
- Reviewed IT system and other documentation
- Reviewed the results of recent vulnerability scans performed by the Information Security Office

We conducted our audit in accordance with guidelines set forth in The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

---

<sup>1</sup>*Texas Government Code §552.139 Exception: Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers– Information is excepted from the requirements of §552.021 (Availability of Public Information) if it is information that relates to computer network security or to the design, operation, or defense of a computer network.*

---

**UT Health Northeast**  
**IT Security Assessment Follow-up Audit**  
**Fiscal Year 2015**

***Audit Results***

Per Texas Government Code §552.139, information about computer vulnerabilities is not subject to public disclosure. Due to the sensitive nature of the audit findings, this report will only include a summarized conclusion based on the audit results.

***Conclusion***

Based on the results of procedures performed, we believe collaboration between the Information Technology and Information Security departments is currently progressing to resolve critical and high-risk vulnerabilities identified by the external consulting firm as well as those subsequently identified in more recent vulnerability assessments and scans. A team from the Information Technology and Information Security Departments has been identified and beginning in April 2015 this team will begin to meet monthly to facilitate review and resolution of existing critical IT vulnerabilities identified as well as any new critical risks identified. Although much progress has been made in resolving the critical vulnerabilities, for some of the high risk vulnerabilities identified resolution is moving at a slower pace due to limited financial and technical resources to both purchase and implement tools, staffing constraints in the Information Security and Information Technology areas and other essential competing priorities.



---

Kris I. Kavasch, Chief Audit Executive

**UT Health Northeast**  
**IT Security Assessment Follow-up Audit**  
**Fiscal Year 2015**

***Summary of Priority Findings***

According to The University of Texas System, a priority finding is 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. Standard factors for determining a priority finding have been established in three categories: namely, Organizational Controls, Quantitative Risks, and Qualitative Risks”.

In view of the above requirements, the IT Security Assessment Follow-up Audit for FY 2015 had no priority findings.