AUDIT REPORT

TO: Mr. Yeman Collier, VP and Chief Information Officer
    Dr. Francisco González-Scarano, Dean of School of Medicine
    Dr. Carlos Rosende, Dean for Clinical Affairs

FROM: Ms. Angela D'Anna, Chief Audit Executive, Internal Audit and Consulting Services

DATE: September 11, 2014

SUBJECT: Departmentally Managed Research Server Security (14-19)

EXECUTIVE SUMMARY

Internal Audit and Consulting Services has examined server security for departmentally managed research servers at UT Health Science Center San Antonio (UTHSCSA). Research servers managed by the departments were located inside and outside of University data centers. The major objective of the audit was to determine whether University security requirements were adhered to. In general, the departmentally managed research servers were managed in accord with the UTHSCSA security requirements. However, approval had not been obtained from the Chief Information Officer for certain departmentally managed research servers located outside of University data centers as required by policy. This audit identified no issues considered priority to the institution.

DETAILED REPORT

Attached is the detailed internal audit report.

AUDIT TEAM

Jaime M. Contreras, Information Systems Manager
Jennifer McGowan, Internal Audit Associate

AUDITING STANDARDS

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

Distribution of this report is limited to appropriate members of University of Texas System and Health Science Center management only. This report is confidential and is exempt from public disclosure under Texas Government Code, Section 552.139.
DISTRIBUTION

Mr. Michael Black, Senior Executive VP and Chief Operating Officer
Dr. Donald Dougherty, Psychiatry, Deputy Chair of Research
Dr. Peter T. Fox, Research Imaging Institute Director
Dr. Victor German, Community Pediatrics Clinical Professor
Dr. Raymond Greenberg, Executive Vice Chancellor for Health Affairs, UT System
Dr. William Henrich, President
Dr. Hui-Ming Tim Huang, Molecular Medicine Chair
Dr. Anthony Infante, Professor Pediatrics-Infectious Diseases
Dr. Victor Jin, Molecular Medicine Associate Professor
Dr. Jack Lancaster, Research Imaging Institute Associate Director
Dr. Murray P. Luber, Psychiatry Chair ad interim
Dr. Thomas C. Mayes, Pediatrics Chair
Dr. Bruce Nicholson, Biochemistry Chair
Mr. Michael Parker, Molecular Medicine Technical Support Analyst
Dr. Brad H. Pollock, Epidemiology and Biostatics Chair
Mr. Michael Peppers, Chief Audit Executive, UT System
Mr. William Sanns, Epidemiology and Biostatics Director of Information Systems
Mr. Michael Schnabel, Chief Information Security Officer
Mr. Lewis Watkins, Chief Information Security Officer, UT System
DETAILED AUDIT REPORT

PURPOSE AND SCOPE

Internal Audit and Consulting Services has examined server security for departmentally managed research servers at UT Health Science Center San Antonio (UTHSCSA). Research servers managed by the departments were located inside and outside of University data centers. The Asset Management System listed 31 departments that appeared to house research servers outside of the data centers. For our review of server security, we selected the eight (8) departments which potentially housed the greatest number of research servers outside of data centers. The major objectives of the audit were to determine whether departmentally managed research servers were located inside or outside of data centers and ascertain whether UTHSCSA security requirements were adhered to.

RESULTS

In general, the departmentally managed research servers were managed in accord with the UTHSCSA security requirements. However, approval had not been obtained from the Chief Information Officer for certain departmentally managed research servers located outside of University data centers as required by UTHSCSA policy. Other opportunities for internal control improvement were also noted.

This audit identified no issues considered priority to the institution. According to Exhibit A of UT System Policy 129 - Internal Audit Activities, a priority audit issue is one that is material to the operation, financial reporting, or legal compliance of the institution.

BACKGROUND

In 2013, a Server Centralization project was undertaken by Information Management Services (IMS) with the purpose of moving department servers to University data centers. The project involved 23 departments that reported they departmentally managed servers. Of the 23 departments, six (6) departments retained the rights to fully manage their servers and five (5) departments continued to substantially manage their servers (with exceptions for backup/patches). Documentation regarding the level of departmental management was captured in service work agreements (SWAs) with IMS. The Server Centralization project improved the risk profile for departmentally managed research servers, resulting in enhanced physical security and opportunities for the departments to purchase backup, change management, and network logging services from IMS.

It is important for the institution to ensure that departmentally managed research servers are managed in accordance with UTHSCSA security requirements. This helps to ensure the security and integrity of research data stored in departmentally managed servers.

Attached are the audit recommendations, management action plans, responsible parties, and anticipated completion dates. These matters are offered for management's consideration in the spirit of continuously improving processes and reducing risks in the organization.
Servers Located Outside of Data Centers

Opportunity for Improvement:

Of the eight (8) departments reviewed, five (5) had departmentally managed research servers located in University data centers and three (3) had servers located outside of data centers; however, approval for servers located outside of data centers had not been formally obtained. We noted the following regarding the research servers located in the departments:

- **Community Pediatrics**: Research servers were located in the Santa Rosa Pavilion building in a locked room that also served as work space for the server administrator. The servers were connected and registered on the Health Science Center (HSC) network but the data had been de-identified.

- **Molecular Medicine**: Research server was located in the South Texas Research Facility within a lab, on a shelf, and used for backups. The server was not connected on the HSC network and the data had been de-identified.

- **Biochemistry**: Research servers were located in a locked room in the Medical School building. The cluster of servers had not been relocated to a data center due to age. The servers were connected and registered on the HSC network in an area segmented from sensitive data and the data had been de-identified.

Health Science Center Policy 5.8.14 (Server Security) requires all servers to be located in approved University data centers and that exceptions be approved by the Vice President and Chief Information Officer (CIO).

Recommendation:

Consideration should be given to housing the research servers in one of the University data centers. If it is not feasible to house the servers in a data center, exception to the HSC requirement should be obtained from the CIO in accordance with HSC policy.

Management's Action Plans:

Departmental management will communicate with Information Management Services (IMS) and determine whether to migrate the servers to a data center or obtain an exception from the CIO.

Responsible Party(s):

- Dr. Victor German, Community Pediatrics Clinical Professor
- Mr. Michael Parker, Molecular Medicine Technical Support Analyst
- Dr. Bruce Nicholson, Biochemistry Chair

Estimated Completion Date(s): 10/31/2014
Service Management Agreements

Opportunity for Improvement:

Certain elements of the Information Management Services (IMS) service management agreements were not clear and as a result, the following gaps in coverage were noted:

- **Research Imaging Institute (RII):** The RII agreement did not include *change management* and only included one level of *logging* (system monitoring *without* Systems Center Operations Manager (SCOM) monitoring). SCOM provides alerts generated based on availability, performance, configuration or certain security situations being identified.

- **Psychiatry:** The agreement did not include *access management services* from IMS.

Insufficient service agreement coverage may result in key security control gaps in access management, logging, and change management (configuration changes).

Recommendation:

The service agreements should be reviewed to determine whether the appropriate coverage has been obtained for the research servers. Furthermore, consideration should be given to simplifying the IMS service management agreements.

Management's Action Plans:

Departmental management will communicate with IMS and determine whether additional services should be included in the service management agreements.

IMS has redeveloped the Server Management Agreement for FY15 which included a ground-up re-write of the entire document.

Responsible Party(s):

Dr. Jack Lancaster, Research Imaging Institute Associate Director  
Dr. Murray P. Luber, Psychiatry Chair *ad interim*  
Mr. Michael Schnabel, Chief Information Security Officer

Estimated Completion Date(s):

10/31/2014 (Research Imaging Institute and Psychiatry)  
Completed (Information Management Services)
Server Administration

Opportunity for Improvement:

Departmental server administrators were not aware of certain HSC security requirements as follows:

- **Research Imaging Institute (RII) and Epidemiology and Biostatics (EpiBio):** The department administrators did not provide evidence that service accounts were registered with the Chief Information Security Officer (CISO). Service accounts are where more than one user shares a sign-on and password. Health Science Center Policy 5.8.4 (Access Control & Password Management) states that service or shared accounts must be approved by the Chief Information Security Officer (CISO) and must be strictly documented and regulated.

- **Community Pediatrics:** The department did not provide evidence that two server administrators had completed the training required in accordance with the HSC Server Security Standard. The HSC Server Security Standard requires server administrators to complete the Technical Service Representative training.

Server administrators are typically granted administrative or special rights to manage departmental servers. Proper server administration is needed to maintain an optimally secure server environment.

Recommendation:

Notification of shared accounts should be given to the CISO so that approval can be obtained in accordance with policy. Additionally, the server administrators should complete the required training.

Management's Action Plans:

Departmental management for RII and EpiBio will communicate with the Information Security Department and confirm whether any of the Linux/Unix accounts fall under the provisions of the shared account policy and obtain approval from the CISO if deemed necessary. Community Pediatrics server administrators will complete and retain documentation of the required training.

Responsible Party(s):

Dr. Jack Lancaster, Research Imaging Institute Associate Director  
Mr. William Sanns, Epidemiology and Biostatics Director of Information Systems  
Dr. Victor German, Community Pediatrics Clinical Professor

Estimated Completion Date(s):

10/31/2014
Security Log Review & Data Backups

Opportunity for Improvement:

Departmental server administrators were not aware of certain HSC security requirements as follows:

- **Community Pediatrics:** Review of security logs focused only on malware and did not include a review of inappropriate access, unsuccessful login attempts or changes to security configuration settings. The department also stored backup media within the designated server room.

- **Molecular Medicine:** The department relied solely on Redundant Array of Independent Disks (RAID). RAID is a data storage virtualization technology that combines multiple disk drive components into a logical unit for data redundancy and is not intended for backup purposes.

The HSC Server Security Standard states:

- Operating system event logging must be enabled for security events such as failed logins, unauthorized connections and unauthorized changes to security configuration settings.
- Backup media must be stored in a secure location at a safe distance from the server.
- The backup plan must ensure that backups are usable and the plan is sufficient to provide the required data protection.

Appropriate logging and monitoring enables detection of inappropriate changes to security settings and inappropriate access attempts. Proper backup and storage for backup media helps to ensure that data can be recovered in the event of a loss or system disruption.

Recommendation:

A more comprehensive review of security logs by the server administrator should be put in place to include review of inappropriate access attempts, failed logins and inappropriate changes to configuration settings. Additionally, backup media should be stored at a location distinct from the original servers. Furthermore, a backup strategy should be established for the servers in Molecular Medicine.

Management's Action Plans:

Community Pediatrics will determine whether to institute a process to log and monitor failed logins and unauthorized connections to the servers or arrange with Information Management Services (IMS) to provide this service. Additionally, backup media will be moved to a separate secure location that is not in the server room. Molecular Medicine will determine whether to establish a backup process or arrange for backup coverage from IMS.

**Responsible Party(s):**  
Dr. Victor German, Community Pediatrics Clinical Professor  
Dr. Victor Jin, Molecular Medicine Associate Professor

**Estimated Completion Date(s):**  
10/31/2014