UTSA. The University of Texas at San Antonio™
AUDITING & CONSULTING SERVICES

UNIX Server Management & Security Internal Audit Report

Project # 2014-32

May 26, 2015

Reviewed by: _____
Dr. Ricardo Romo
President

EXECUTIVE SUMMARY

Objectives:
Provide a limited independent assessment of the implementation and operating effectiveness of UNIX operating system security configuration and management.

Background/Scope:
UNIX is a computer operating system and the base software that controls a computer system and its peripherals. It provides the foundation mechanisms for booting a computer, logging in, running applications, storing and retrieving files. UNIX was not designed to be a secure operating system; rather, it was designed to be flexible, open, and portable. Most vendors have improved security over the years; however, UNIX requires significant system administrator knowledge to run the system securely.

UTSA currently has an approximate inventory of 128 UNIX server environments (95 production and 33 development/test environments) with 3 full-time support staff assigned the administrative duties of maintaining these environments.
The scope of our review included those UNIX environments that supported the following business applications and data repositories:
- ➢ BANNER (Student Information System)
- ➢ Degree Works
- ➢ UTSA Web-sites
- ➢ Identity Management System

Conclusion:
Internal Audit contracted with an outside consultant, CanAudit, to perform a security evaluation on a sample of UTSA's UNIX servers using their Sys-Secure system. The consultant's reports indicated a satisfactory level of security on the UNIX servers reviewed. The Enterprise Services Team should be commended for their efforts to provide a secure UNIX infrastructure. We want to thank them for their assistance with the audit and encourage them to continue with the implementation of the security guidelines and standard build templates. By utilizing the results obtained from this audit and the additional information provided by the consultant (CanAudit), the process should continue to improve existing UNIX systems and future implementations.

AUDIT RESULTS

Objective: Provide a limited independent assessment of the implementation and operating effectiveness of UNIX operating system security configuration and management.

|	
UNIX Server Assessments	Internal Audit contracted with an outside consultant, CanAudit, to perform a security evaluation on a sample of UTSA's UNIX servers using their Sys-Secure system. Sys-Secure is an easy inexpensive way to identify, track and resolve security issues. The Sys-Secure database includes over a thousand rules for identifying risk and exposures in a system. The consultant provided reports comparing UTSA's UNIX security environment to other organizations and provided a raw scoring based on the initial results. Each Sys-Secure report provided both informational items and items noted as potential issues. Due to the size of each report (100+ pages), Internal Audit reviewed each report and extracted those items identified as potential issues into separate individual spreadsheets. The majority of the issues were identified to be low risk with a couple issues being ranked as medium. Internal Audit worked with the Enterprise Infrastructure Team to review the potential issues over the course of 3 months to identify false positives, compensating controls, immediate corrections to be made and action plans for updating security guidelines and implementation templates. All items remaining to be addressed are low risk. No audit recommendations are required for this environment at this time.
Conclusion	Internal Audit contracted with an outside consultant, CanAudit, to perform a security evaluation on a sample of UTSA's UNIX servers using their Sys-Secure system. The consultant's reports indicated a satisfactory level of security on the UNIX servers reviewed. The Enterprise Services Team should be commended for their efforts to provide a secure UNIX infrastructure. We want to thank them for their assistance with the audit and encourage them to continue with the implementation of the security guidelines and standard build templates. By utilizing the results obtained from this audit and the additional information provided by the consultant (CanAudit), the process should continue to improve existing systems and future implementations.

This engagement was conducted in accordance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

J. Richard Dawson
Institution Chief Audit Executive
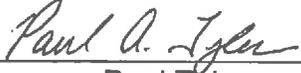
Paul Tyler
Director, Auditing and
Consulting Services

Carol Rapps
Audit Manager, Information Systems