THE UNIVERSITY OF TEXAS-PAN AMERICAN
OFFICE OF AUDITS & CONSULTING SERVICES

Computer Administrative Rights

Report No. 15-14
August 31, 2015

Dr. Havidán Rodríguez, Interim President
The University of Texas-Pan American
1201 W. University Drive
Edinburg, TX  78539

Dear Dr. Rodríguez,

As part of our fiscal year 2015 Audit Plan, we completed a risk based audit of Computer Administrative Rights. The objective of this audit was to evaluate the granting of local administrative rights to desktops and laptops. The scope of the audit consisted of current procedures and users with administrative rights accounts.

Overall, we concluded that the granting of users administrative rights accounts was not managed appropriately. We determined that there was no documentation maintained to support when the administrative rights accounts were granted and for what purpose. With the creation of the new University, the process of granting users administrative rights accounts has changed and a new, controlled process will be implemented. The detailed report is attached for your review.

We appreciate the courtesy and cooperation received from management and staff during our audit.

Sincerely,

Eloy R. Alaniz, Jr., CPA, CIA, CISA
Chief Audit Executive
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>1</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT OBJECTIVE</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT SCOPE AND METHODOLOGY</td>
<td>3</td>
</tr>
<tr>
<td>AUDIT RESULTS</td>
<td>3</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>4</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Information security is a major concern for universities. Universities collect and maintain confidential and/or sensitive information that must be protected. One method of protecting this information is by properly managing the administrative rights accounts of desktop and laptop computers. By properly managing these accounts, organizations can mitigate installation of malware and unlicensed software, the disabling of security settings and hackers penetrating protected networks where private and sensitive information resides. People who are granted administrative rights accounts are able to change security settings and existing user accounts, install software and hardware, access all computer files, and create user accounts. These accounts are intended for employees that maintain and fix computers, but are also granted to faculty and staff.

According to University of Texas System (UTS) 165 (Information Resources Use and Security Policy), Standard 5: Administrative/Special Access Account institutions must adopt procedures to ensure that all administrative/special access accounts are preauthorized and used only for their intended administrative purpose.

The objective of the audit was to evaluate the granting of local administrative rights to desktops and laptops. There were 4,639 computers with administrative rights accounts granted to users, and we tested 95 of those accounts.

Overall, we concluded that the granting of users administrative rights accounts was not managed appropriately. We determined that there was no documentation maintained to support when the administrative rights accounts were granted and for what purpose. We observed the following:

- All, but one, of the accounts tested lacked documentation.
- 68 of the accounts tested belonged to employees that did not have an information technology position.

Recently, the process to grant users administrative rights accounts was reviewed and appropriately changed. However, as indicated above, many users continue to maintain those administrative rights without justification.

Beginning on September 1, 2015, The University of Texas at Brownsville and The University of Texas – Pan American (UTPA) will consolidate to create The University of Texas Rio Grande Valley (UTRGV). For UTRGV, all users requiring administrative rights accounts must request and receive approval from the Office of Chief Information Security Officer (OCISO). The Office of Internal Audits will follow-up with the UTRGV responsible party for this area to ensure that the issues identified in this audit are addressed and mitigated.
BACKGROUND

Daily University processes depend greatly on technology. Students and University employees utilize this technology through desktops, laptops, tablets, and personal devices. The University employs several methods to protect these devices such as anti-virus software, encryption, and strong passwords. This protection may be rendered useless if the administrative access to devices is not properly managed. According to UTS 165 (Information Resources Use and Security Policy) management of special access includes, but not limited to:

- Ensure that accounts with administrative access are only used for their intended administrative purposes.
- Administrative access accounts may be used to perform investigations related to potential misuse of information resources only under the supervision of the information security office.
- Administrative access accounts must adhere to the University password requirements.
- University departments must submit to the information security office a list of administrative contacts for any systems connected to and application running on the University network.
- All information technology professionals acting as custodians of University information must acknowledge their custodial role and responsibilities.
- The password for a shared administrator/special access account must change when any individual knowing the password leaves the department or the University, or changes role, or upon a change in the vendor personnel assigned to University contracts and must follow the University password requirements.
- For each secured system there must be a password escrow procedure in place to enable someone other than the administrator to gain access to the system in an emergency situation.
- When administrative accounts are needed for auditing, software development, software installation, or other defined need, they:
  - Must be authorized by the appropriate department head or owner;
  - Must be created with an expiration date; and
  - Must be removed when work is complete.

In September 2015, The University of Texas Pan American and The University of Texas at Brownsville will combine its talent to create The University of Texas Rio Grande Valley. Currently, UTPA and UTRGV have an interim Chief Information Security Officer (CISO), and a search for a permanent CISO is underway.

AUDIT OBJECTIVE

The objective of this audit was to evaluate the granting of local administrative rights to desktops and laptops.
AUDIT SCOPE & METHODOLOGY

The scope of the audit consisted of current procedures and users with administrative rights accounts. To accomplish the audit objective, we performed the following:

- Gained an understanding of the process to obtain an administrative rights account.
- Gained an understanding of applicable state statutes and University policies.
- Interviewed staff from the Office of the Chief Information Security Officer, Help Desk, and Application and Computing Services department.
- Tested the administrative rights accounts with applicable policies and procedures.

The audit was conducted in accordance with guidelines set forth in The University of Texas System’s Policy 129 and The Institute of Internal Auditor’s International Standards for the Professional Practice of Internal Auditing.

AUDIT RESULTS

Request Process

The current process to grant users with administrative rights is initiated with a call to the University Help Desk. The Help Desk will then refer the requestor to the Desktop and Portable Computer Security Standard policy. The requestor will fill out a form and submit it to the OCISO. If appropriate justification for administrative rights exists, the OCISO will approve and create a service request in the service management system (ServiceNow) to have the Help Desk grant the requestor administrative rights to their computers. If the request is denied, the OCISO will inform the requestor via email or phone.

Documentation for administrative rights requests is maintained in several places. ServiceNow is the current system used by the Help Desk to document all service requests, including administrative rights requests. Only two approved requests are documented in ServiceNow since its implementation in 2014. Altiris was the system used before ServiceNow.

The OCISO keeps hardcopy forms for administrative rights requests. These forms are part of the information security exceptions forms. The OCISO only had sixteen forms with approved administrative rights requests, including the two approved requests documented in ServiceNow.

We interviewed the security engineer from the OCISO and the Help Desk supervisor. Both employees agreed that the number of approvals for administrative rights has drastically decreased in recent months.

Accounts

A test was performed to determine if existing administrative rights accounts were requested through a formal request process that included the purpose for the account and proper approvals.
The sample selected for this test included 95 computers (2%) from a list of 4,639 computers with administrative rights accounts. The sample was randomly selected. The list of computers whose users have been granted administrative rights accounts was provided by the Application and Computing Services department. For this test we reviewed documentation from the Altiris and ServiceNow systems used by the Help Desk and information security exception forms kept by the OCISO.

We were unable to determine when these accounts were granted. 94 out of 95 administrative rights accounts tested did not have formal request documented. Only one (1) account request was documented in Altiris and while it included the purpose, it did not include proper approval.

**Account Maintenance**

A test was performed to determine if the list of administrative rights was accurate, accounts with administrative rights belonged to current employees, and job duties merited administrative rights. The sample selected for this test was the same as the one in the previous section. For this test we reviewed asset, employee, and job position documentation from Oracle.

All computers tested were listed in the University’s inventory. 80 out of the 95 computers in the test sample had administrative rights accounts that were tied to current University employees, and the remaining were not tied to individual employees and were for department use. 68 out of the 80 computers had administrative rights accounts that belonged to employees that did not have information technology positions. 12 computers had administrative rights accounts that belonged to employees with information technology positions.

**CONCLUSION**

Overall, we concluded that the granting of users administrative rights accounts was not managed appropriately. We determined that there was no documentation maintained to support when the administrative rights accounts were granted and for what purpose. With the creation of the new University, the process of granting users administrative rights accounts has changed and a new, controlled process will be implemented.

Isabel Benavides CIA, CGAP, CFE
Director, Audits and Consulting Services

Jose Gomez, MS
Senior Information Technology Auditor