AUDIT OF INTERNET NATIVE BANNER USER ACCESS

THE UNIVERSITY OF NEW MEXICO

Report 2018-06
August 15, 2018

THE UNIVERSITY OF
NEW MEXICO

Audit and Compliance Committee Members

Thomas Clifford, Chair
Garrett Adcock, Vice Chair
Lt. Gen. Bradley Hosmer

Audit Staff

Manu Patel, Internal Audit Director
Chien-Chih Yeh, Internal Audit Manager
Lisa Wauneka, Information Systems Auditor
Victor Griego, Senior Auditor

CONTENTS

ABBREVIATIONS

BAA	Banner Authorization Administrator System
Banner	Internet Native Banner (Banner) Information system
BAR	Banner Authorization Request System
ERP	Enterprise Resources Planning
HR	Human Resources
Internal Audit	Internal Audit Department
ISACA	Information Systems Audit and Control Association
UNM IT	Information Technology
Oracle	Oracle Relational Database Management System
University	The University of New Mexico
UAP	University Administrative Policies and Procedures Manual
UNM	The University of New Mexico
UNMH	University of New Mexico Hospital

Internal Audit found users with excessive access to modify data in Finance, Human Resources, Student, and Student Financial Aid modules. The access would be considered excessive based on the user's job duties and department.

Banner payroll time keeper and time approver permissions are sometimes given to the same employee. Employees have permissions for both of these functions, giving these employees the ability to enter and approve time.

EXECUTIVE SUMMARY

The Internal Audit Department (Internal Audit) conducted an audit of selected general and application system controls relating to the University of New Mexico's (University) Internet Native Banner (Banner) information system. Banner is an integrated suite of administrative applications used university-wide. The University has implemented the Finance, Student, Financial Aid, General, Budget Development, and Human Resources modules of Banner.

BANNER USER ACCESS

Finance -Payroll Timekeeping Segregation of Duties

Banner payroll time keeper (data entry for timesheet submission) and time approver permissions are sometimes given to the same employee. Employees have permissions for both of these functions, giving these employees the ability to enter and approve time. This was allowed so small departments with few employees can meet payroll processing deadlines. Employees will not get paid unless time is entered and approved. Best practices pertaining to the payroll accounting cycle recommend that payroll time entry and payroll approver duties should be segregated. This is also a preventive internal control because review by a different employee may identify errors and irregularities in time reporting before payroll is processed.

Banner Segregation of Duties – Information Technology Services Programmers

Programmers should not have access into production. Changes in production should be made through the change control process. Programmers may be given access to the database in emergencies in accordance with established change control procedures.

Programmers have access to modify Banner data.

Internal Audit determined that there were 18 locked accounts with a time period between 6 and 27 days from the employee's termination date to the date the account was disabled.

TIMELY DISABLING OF BANNER ACCESS

The Banner Security Administrators have procedures in place for disabling user accounts, which disables access to Banner, when employees are terminated or transfer departments. In these instances, access to Banner should be disabled in a timely manner. When employee access to Banner is not disabled in a timely manner after an employee is terminated, it is because employee terminations are not being entered into Banner in a timely manner, which in turn causes the untimely disabling of user access into Banner.

Although Internal Audit did not note access to Banner subsequent to any of the employees' termination dates, the risk of unauthorized access to finance, payroll, human resources, and financial aid forms upon termination is increased.

UNM IT BANNER DATACENTER PHYSICAL SECURITY

Internal Audit performed audit procedures to determine if there is adequate physical security to protect the servers which contain Banner data within the UNM IT datacenter. Banner servers are located in one room in the UNM IT datacenter that can be accessed through only one door using a badge system. Physical security controls are necessary to ensure unauthorized individuals do not obtain access to the Banner datacenter.

Vendor and Physical Plant Department employees have unsupervised access to the datacenter to perform maintenance. Internal Audit also found that employees who are not on the badge access list are obtaining access to the Banner datacenter.

Conclusion

The following is a summary of recommendations made in the report.

Physical Security best practices suggest non-IT personnel, such as Physical Plant Department employees and vendors, be escorted to and from a restricted area and supervised while in the restricted area.

1. Finance -Payroll Timekeeping Segregation of Duties. UAP 2610 Time and Leave Reporting should be revised to clarify that time keeper and time approver functions should be segregated and the same employee should not perform both functions and in no case should an employee enter and approve their own time. Employees who are both timekeepers and time approvers should have their approval access removed or compensating controls should be developed if the access is necessary for business purposes.

2. Banner Segregation of Duties - IT Programmers. UNM IT should remove programmer access into production. Changes in production should be made through the change control process. Programmers may be given access to the database in emergencies in accordance with established change control procedures.

3. Timely Disabling of Banner Access. The Vice President of Human Resources and the University Controller should work together to ensure that employee separations are processed in a timely manner.

4. UNM IT Banner Datacenter Physical Security. Non-IT personnel and/or visitors that access the Banner datacenter should be supervised at all times or compensating controls should be developed to control the access of these individuals. In addition, accurate authorized access listings should be maintained and updated on a regular basis and user access should be reviewed on a regular basis.

INTRODUCTION

BACKGROUND

Banner, an integrated suite of administrative applications, is the core administrative system at the University. Consisting of the Banner modules for Accounts Receivable, Advancement, Finance, Financial Aid, General, Human Resources (HR), Position Control, and Student, the modules run on a single database, the Oracle Relational Database Management System (Oracle). Banner application security is built on top of Oracle database security. Due to this integrated design, both Banner security and Oracle database security systems must be properly administered and secured to protect the systems and data.

Banner is the most critical information system for the core administrative functions of the University. Banner houses sensitive student, employee, and financial data protected by various Federal laws including the Family Educational Rights and Privacy Act and the Gramm-Leach-Bliley Act. Adequate Banner security is critical to the University to ensure the information system functions as intended and to protect the sensitive information processed and stored by Banner.

Banner is administered by UNM Information Technologies (UNM IT). UNM IT maintains the Banner Authorizations Request (BAR) system and the Banner Authorization Administrator System (BAA). The BAR is employed by Banner users to request access to Banner and other applications. The BAA is used by Banner Security Administrators to administer UNM employee roles, privileges, classes, and other Banner access. Access requests are submitted by the user, and are approved by the user's supervisor and the Data Owner of each access role before users are granted access to Banner. Termination of user access is also performed in the BAR. Users may be terminated based on supervisor request or by an automated process in the BAR which based on an employee's termination date entered into Banner, notifies the Banner Security Administrators that the employee's Banner access should be disabled. The BAR system creates an audit trail for requests and approvals.

Banner security functions are performed by Banner Security Administrators in HR, Controllers and Enrollment Management. Other users within UNM IT can also perform Banner Security administration functions.

Briefly, Banner gives users access to perform their job duties based on Oracle's role-level privileges. The user is granted access to an Oracle role. The Oracle role grants the Oracle user privileges to allow the user to logon to the Oracle database. The user is assigned a Banner access role which is based on the user's job responsibilities. The role is comprised of Banner classes, which are groupings of different objects. These classes grant the user access to objects such as forms. For example, an Accounts Payable Clerk is granted an Oracle role to logon to Oracle and the clerk is granted the Banner access role for Accounts Payable Clerks. This Banner access role is assigned classes which allow the Accounts Payable Clerk to input vendor invoices for payment, review vendors, review vendor history, etc.

PURPOSE

The audit was selected as part of the Internal Audit work plan. Our audit objectives are to determine compliance with best practices for Banner general user access management and datacenter physical security of the UNM IT datacenter that houses the Banner servers.

SCOPE and PROCEDURES

The audit focused on user access management for general users and UNM IT datacenter physical security. The review of general user access encompassed the user access data for the period April 2015 through February 2016. Superusers, employees with extensive access to the Banner system or data, and other Oracle access controls will be reviewed in a separate audit.

The audit consisted of interviews, reviews of documentation, a tour of the Banner datacenter, a review of access into the Banner datacenter, a statistical sample of Banner user's access, and a review of user access to modify data in important Banner forms. Internal Audit completed audit fieldwork in February 2016. Criteria for the audit was developed using the following sources.

- Oracle Database 3rd Edition, Security, Audit and Control Features
- Banner Technical Reference Manual
- Banner General Security Administration Handbook
- Association of College and University Auditors Banner Access Audit Tool
- 2015-2016 Federal Student Aid Handbook, Volume 4—Processing Aid and Managing FSA Funds, 2015-2016, A School's Financial Management Systems, Appendix B
- UNM IT and IA have agreed to survey the practices of the following peer institutions for inclusion in criteria: Texas Tech University, Temple University, and the University of Illinois at Urbana-Champaign.
- University Administrative Policies and Procedures Manual (UAP)

The audit scope included only Banner. It did not include the following Banner-related components: computer hardware, Banner operating system software, Banner interfaces, Banner Self-Service, or associated Banner systems such as Xtender, MyReports, HRReports or ePrint.

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

Banner User Access

User access permissions for Banner should be requested by the user, approved by the user's supervisor, approved by the Data Owners, and implemented by Banner Security Administrators. Users should be granted the minimum permissions needed to perform their job duties. User access should be disabled immediately upon termination and should be modified when a user changes job positions. Permissions granted to the users should not violate segregation of duties internal control requirements.

A fundamental element of internal control is the segregation of certain key duties. The basic idea underlying segregation of duties is that no employee or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated include:

- Custody of assets
- Authorization or approval of related transactions affecting those assets
- Recording or reporting of related transactions, and
- Execution of the transaction or transaction activity

An essential feature of segregation of duties/responsibilities within an organization is that no one employee or group of employees has exclusive control over any transaction or group of transactions. Ideally, a single employee would have access to only one of the four incompatible duties.

There are also preventive and detective internal controls. Preventive internal controls will ensure that the control will not be bypassed. These controls include the review and approval of purchases before the purchase, review and approval of timesheets before the employee is paid, approval of the access requested by a user to a system before the access is granted, and use of user names and passwords before access to data is granted to a user. Detective controls occur after the transaction or activity has occurred, such as cash counts, reconciliations, monitoring actual expenditures against budget, and comparing transactions on reports to actual documents.

Internal Audit sampled 76 users which included reviewing the appropriateness of the user's access based on the user's job description and department, and ensuring the user access was approved by the Data Owners. The review of user access to modify data in significant Banner forms also included reviewing the appropriateness of the user's access based on the user's job description and department.

Employees should only have the access required to perform their job duties. Additional access may result in the unauthorized use, unintentional modification, disclosure, damage, or loss of the information system or information system data.

Internal Audit reviewed, tested, and assessed UNM Banner access roles to determine if segregations of duties issues existed for key UNM accounting cycles, financial aid, and information technology. Internal Audit used creditable sources including BDO Consulting, the Information Systems Audit and Control Association (ISACA), and 2015-2016 Federal Student Aid Handbook, Volume 4 to assist in the assessment of segregation of duties within the UNM functions. The following user access exceptions were identified by reviewing users selected through a statistical sample of Banner users and reviewing modify user access to significant Banner forms.

Finance -Payroll Timekeeping Segregation of Duties

Banner payroll Time Keeper (data entry for timesheet submission) and Time Approver roles are sometimes given to the same employee. Employees have permissions for both of these functions, giving these employees the ability to enter and approve time. This was allowed so small departments with few employees can meet payroll processing deadlines. Employees will not get paid unless time is entered and approved.

UAP 2610 Time and Leave Reporting states that there are two roles in the timekeeping process, the time keeper (Banner Time Keeper role) and the department administrator or authorized administrator (Banner Time Approver role). The timekeeper enters exempt employee's annual and sick time and timesheet information for biweekly employees. The authorized administrator approves electronic time input and conducts a full reconciliation of the internal timesheets and the electronic time reports and signs the reconciliations. In reading the policy it implies that the timekeeper and authorized administrator are not the same employee when in reality it can be the same employee performing all these functions.

Best practices pertaining to the payroll accounting cycle recommend that payroll time entry and payroll approver duties should be segregated. This is also a preventive internal control because review by a different employee may identify errors and irregularities in time reporting before payroll is processed. Hours worked should be reviewed and approved by the employee's supervisor prior to being recorded or transmitted to the payroll department. By combining these duties, employees may have the ability to modify their paychecks by reporting unearned overtime or under reporting sick and annual leave. In addition, timesheet errors on other employee timecards may not be identified without a secondary review.

Internal Audit contacted several peer institutions to compare UNM processes to our peer institutions processes. Temple University uses Kronos Time Keeping to record all payroll hours for hourly employees using time clocks. The timekeeper approves the bi-weekly employee's time. For exempt employees, the timekeeper enters only exception time for vacation, sick, holiday, etc. Temple did not indicate whether the timekeeper and time approver for exempt employees is the same employee or a different employee.

The University of Illinois employees, using web time entry, or originators, using department time entry, enter the employee's time into Banner time entry forms. The approver reviews and approves the information entered. The approver cannot approve their own time.

Internal Audit found that five of 76 employees tested had both time keeper and time approver roles.

1. Psychiatry Department – Administrative Coordinator
2. Psychology Department – Sr. Fiscal Services Tech
3. Experimental Therapeutics – Unit Administrator 2
4. Physical Property Department – Accountant 2
5. Music Department – Coord, Theater/Concert Production

Recommendation 1

UAP 2610 Time and Leave Reporting should be revised to clarify that time keeper and time approver functions should be segregated and the same employee should not perform both functions and in no case should an employee enter and approve their own time. Employees who are both timekeepers and time approvers should have their approval access removed or compensating controls should be developed if the access is necessary for business purposes.

Response from the University Controller

Action Items
Targeted Completion Date: *June 30, 2016*
Assigned to: *University Controller*
Corrective Action Planned: *The Financial Services Division will work with the UNM Policy Office to draft revisions to UNM Policy 2610 indicating that employees should not approve their own time, and segregation of duties between the timekeeper and approver roles is necessary and compensating controls should be in place if there are necessary business needs for an employee to have both a timekeeping and approver role (example: an employee has a primary timekeeper role, but also has an approver role because they serve as a backup approver.)*

Student - Registration Additional Fees Form

This form provides an individual with the ability to add additional charges to the student registration fee assessment. It can also credit a student's account.

1. One employee – Valencia County Branch Non-credit Teacher has access to add or remove charges to a student account. This employee who does not work in a student area has modify access to this form. It does not appear that this employee should have this ability.
2. One employee - Gallup Branch, Manager Business Services. This employee has modify access to this form and should not have both Finance and Student duties.
3. One employee - School of Medicine, Biomedical Research Education Program, Senior Program Manager. This employee who does not work in a student area has modify access to this form. It does not appear that this employee should have this ability.
4. One employee - Taos Branch, Enrollment Services Representative. This Branch employee has access to Financial Aid, Admissions, and Registration forms. This user appears to have incompatible job duties and has modify access to this form.
5. One employee - Taos Branch, Director, Student Affairs. This Branch employee has access to Financial Aid, Admissions, and Registration forms. This user appears to have incompatible job duties and has modify access to this form.

Recommendation 2

Employees with access to this form from areas other than Enrollment Management should have their modify data access removed or compensating controls should be developed if the access is necessary for business purposes.

Response from the Associate Vice President of Enrollment Management

Action Items
Targeted Completion Date: *June 30, 2016*
Assigned to: *Associate Vice President of Enrollment Management*
Corrective Action Planned: *Access to this form is intricately woven into a primary student role. To remove this access would require excessive resources to extract from currently deployed roles. Enrollment Management will develop compensating control through reports to monitor any adjustments made through this access.*

Audit Note: *This access is needed specifically for small departments and branches. Internal Audit will follow-up to determine if compensating controls through reports has been developed.*

Student Financial Aid Modify Data Access

The Federal Student Aid Handbook, Volume 4 - Processing Aid and Managing FSA Funds, 2015-2016, A School's Financial Management Systems, Appendix B, states that systems should also have controls that prevent cross-functional tampering. For example, according to the Handbook, Financial Aid Office employees should not be able to change data elements that are entered by the Registrar's Office.

Conversely, employees from areas other than Financial Aid should not have the ability to modify data in Student Financial Aid. Internal Audit found employees in departments other than Student Financial Aid with the ability to modify Student Financial Aid data.

Employees should only have the access required to perform their job duties. Additional access may result in the unauthorized use, unintentional modification, disclosure, damage, or loss of the information system or information system data.

Student Financial Aid – Applicant Requirements Form

This access should be restricted to employees in Financial Aid, as this form controls the requirements a student must complete to receive aid. Internal Audit found 17 non-Student Financial Aid employees who have modify access to this form.

1. Three employees - American Indian Student Services
2. Two employees - El Centro de la Raza
3. One employees - Los Alamos Branch
4. Three employees - Taos Branch
5. One employee - Taos Branch, Enrollment Services Representative. This Branch employee has access to Financial Aid, Admissions and Registration forms. This user may have incompatible job duties.
6. One employee - Taos Branch, Director, Student Affairs. This Branch employee has access to Financial Aid, Admissions, and Registration forms. This user may have incompatible job duties.
7. Six employees - Valencia County Branch

Recommendation 3

Employees with access to this form from areas other than Financial Aid should have their modify data access removed or compensating controls should be developed if the access is necessary for business purposes.

Response from the Associate Vice President of Enrollment Management

Action Items
Targeted Completion Date: *June 30, 2016*
Assigned to: *Associate Vice President of Enrollment Management*
Corrective Action Planned: *Enrollment Management will develop compensating control through reports to monitor any adjustments made through this access.*
Audit Note: *This access is needed specifically for small departments and branches. Internal Audit will follow-up to determine if compensating controls through reports has been developed.*

Student Financial Aid – Award Form

This form displays the various financial aid awards a student receives. It also allows users to override system controls, for example, awards that exceed unmet need, fund limits, and tracking requirements. Since a user can override system controls, only Financial Aid users should have access to this form. Internal Audit found three non-Student Financial Aid employees who have modify access to this form.

1. Two employees - American Indian Student Services
2. One employee - Taos Branch, Business Manager

Recommendation 4

Employees with access to this form from areas other than Financial Aid should have their modify data access removed or compensating controls should be developed if the access is necessary for business purposes.

Response from the Associate Vice President of Enrollment Management

Action Items
Targeted Completion Date: *June 30, 2016*
Assigned to: *Associate Vice President of Enrollment Management*
Corrective Action Planned: *Enrollment Management will develop compensating control through reports to monitor any adjustments made through this access.*
Audit Note: *This access is needed specifically for small departments and branches. Internal Audit will follow-up to determine if compensating controls through reports has been developed.*

Student Financial Aid – Record Maintenance Form

This form is used to review and change most of the important aspects of a student's financial aid record. This form displays and allows a user to update: award detail, satisfactory academic progress, budget components, Pell status, and need analysis information. Internal Audit found three non-Student Financial Aid employees who have modify access to this form.

1. Two employees - American Indian Student Services
2. One employee - Taos Branch, Business Manager

Recommendation 5

Employees with access to this form from areas other than Financial Aid should have their modify data access removed or compensating controls should be developed if the access is necessary for business purposes.

Response from the Associate Vice President of Enrollment Management

Action Items
Targeted Completion Date: *June 30, 2016*
Assigned to: *Associate Vice President of Enrollment Management*
Corrective Action Planned: *Enrollment Management will develop compensating control through reports to monitor any adjustments made through this access.*

Audit Note: *This access is needed specifically for small departments and branches. Internal Audit will follow-up to determine if compensating controls through reports has been developed.*

Banner Segregation of Duties - IT Programmers

Programmers have access to modify Banner data. Programmers should not have access into production.

According to ISACA Security, Audit and Control Features Oracle Database 3rd Edition, 10. Access Control Roles:

> At a minimum, security administrators, DBAs, production support personnel and application developers should use individual user accounts assigned to the appropriate role. The security administrator role should have access to security and audit related functions only. Ideally, these tasks should never have access to the data; therefore no privileges would be granted on SELECT, INSERT or DELETE in those tablespaces. The DBA role should have access to all database functions with the exception of security and audit… A production support role should be assigned the minimum level of privileges required for developers to perform production support and application troubleshooting functions; however, they should not be able to change the data on the system and should only be granted access to sensitive data to the extent authorized by the appropriate data owner. The security administrator should work in conjunction with the application development team to determine the privileges required to perform production support functions. In all cases, access to core application tables should be restricted to the DBA to protect the integrity of the system and the enterprise's support contract for ERP systems and other off-the-shelf systems. Any changes to data (INSERT, UPDATE and DELETE privileges) should follow the standards of the software vendor, which typically only suggest changes to core data via scripts developed by the software vendor.

Excessive access may result in the unauthorized use, unintentional modification, disclosure, damage, or loss of the information system or information system data.

Recommendation 6

UNM IT should remove programmer access into production. Changes in production should be made through the change control process. Programmers may be given access to the database in emergencies in accordance with established change control procedures.

Response from the Chief Information Officer

Action Items
Targeted Completion Date: *March 2016*
Assigned to: *Chief Information Officer*
Corrective Action Planned: *IT agrees that limiting programmer access into production should be standard practice. Due to the nature of the Banner software, there are functions that can only be accomplished through direct update of the database, and in those cases business offices and data stewards will request that programmers be given the data update privileges necessary to make those changes.* *As noted in a previous audit, changes to production data are documented in the IT incident management ticketing system. Business office staff enter requests for data updates and receive confirmation when the change has been made and the results are available for review.* *IT continues to use a layered approach to programmer access that limits database access to only those programmers who regularly receive update requests or perform regular maintenance on the database. Programmer access needs are documented, approved by all affected data stewards, regularly reviewed for appropriateness, and removed immediately when staff leave IT or UNM.* *With the move to a new ticketing system (Help.UNM), additional functionality has become available for tracking and managing changes. Applications is currently conducting an evaluation of the expanded change management capabilities and its applicability to improving the tracking and managing of changes to production data. We expect the initial evaluation of change management functionality in Help.UNM to be completed in March, 2016, and, depending on outcomes, we will proceed with the development of a plan for an enhanced change control process.*
Audit Note: *The response will be reviewed when changes controls are enhanced.*

Timely Disabling of Banner Access

The Banner Security Administrators have procedures in place for disabling Banner user accounts when employees terminate or transfer departments. In these instances, Banner user accounts should be disabled in a timely manner to ensure terminated employees are not accessing Banner.

Banner user accounts are disabled by the Banner Security Administrators based on either a supervisors request or by an automated process in the BAR. The automated process using the employee's termination date entered into Banner, notifies the Banner Security Administrators that the employee's Banner user access should be disabled.

Internal Audit performed audit procedures to determine if Banner user accounts are disabled in a timely manner upon an employee's termination by testing all the 98 Banner user accounts disabled between April 1, 2015 and August 31, 2015. Internal Audit found the following.

No. of Days Taken to Disable Banner Account After Employee Term Date	Number of Accounts	Percentage of Accounts
6 to 27	18	18%
1 to 5	36	37%
On or before employees term date	44	45%
Total Accounts	**98**	**100%**

Internal Audit performed further testing of the 18 Banner user accounts disabled 6 to 27 days after the employee's termination date. Internal Audit discovered that three of the 18 accounts were disabled due to the employee's involuntary separation from UNM. These accounts should have been disabled immediately. The time period between termination date and disable date is as follows.

Number of Days Between Employee Termination Date and the Date the Banner User Account was Disabled			
No. of Days	**Department**	**Job Description**	**Involuntary Separation**
6	Global Education Office	Student Intermediate Level	
6	Psychology Department	Admin Assistant 2	
6	Internal Medicine	Admin Assistant 3	
6	HSC Compliance	Compliance Specialist	Yes
6	Family Community Medicine	Coord, Student Services	
7	Family Community Medicine	Admin Assistant 3	Yes
7	Center for High Tech Materials	Program Coordinator	
9	Los Alamos Branch	Assistant Professor	
10	College of Pharmacy	Clinician Ed–Asst. Professor	
10	Office of Equal Opportunity	Compliance Specialist	
11	Women's Center	Dir, Women's Center	
11	Internal Medicine	Program Coordinator	
13	Taos Branch	Student Program Advisor	
14	CAPS	Dir, Academic Support	
18	HR Finance & Business Services	Admin Assistant 1	
24	Transportation Support	Field Supv, Bus Services	
27	Veteran's Outreach	Student Advanced Level	Yes
27	RLSH Operations	Student Intermediate Level	

Internal Audit also found that the delay in removing the Banner user access is attributable to delays in terminating employees in the HR Banner Employee Job Form. Of the 18 Banner user accounts disabled 6 to 27 days after the employee's termination date, the entry of the employee termination date was performed 4 to 14 days after the employee's actual termination date. This delay in entering the employee's termination date in Banner is the cause of the delay in disabling the Banner user account.

Although Internal Audit did not note access to Banner by any of the 18 employees subsequent to the employees' termination dates, the risk of unauthorized access to finance, payroll, human resources, and financial aid data upon termination is increased. Allowing terminated users access to Banner may result in the unauthorized use, unintentional modification, disclosure, damage, or loss of the information system or information system data.

Banner access should be updated in the University's system on a timely basis. Based on industry standards, the appropriate disabling of access within Banner would occur within a reasonable

time. Temple University has different standards for disabling Banner access based on whether the termination is voluntary or involuntary. Banner access is disabled for voluntary employee terminations on the night of the employee's last pay cycle. Banner access for involuntary terminations is disabled using a pre-programmed e-mail sent to the security officers after the nightly interface is run; or for immediate terminations, HR contacts the security officers for immediate revocation.

Recommendation 7

The Vice President of Human Resources and the University Controller should work together to ensure that employee separations are processed in a timely manner.

Response from the Vice President of Human Resources and the University Controller

Action Items
Targeted Completion Date: *July 1, 2017*
Assigned to: *Vice President of Human Resources and the University Controller*
Corrective Action Planned: *Unfortunately, this is no longer an issue of technical programming and security administrator monitoring, but is an issue with departments processing employee separations in a timely manner. In collaboration with Human Resources, management will work to have improved processes in place by July 1, 2017, balancing existing resource constraints and other competing regulatory and compliance requirements and initiatives. The success in meeting this recommendation is fully dependent on the commitment and support from Executive Leadership of the University to require each of their areas to be in compliance with established procedures, processes, practices and requirements.*

UNM IT Banner Datacenter Physical Security

Internal Audit performed audit procedures to determine if there is adequate physical security to protect Banner data within the UNM IT datacenter. Servers that contain Banner data are located in one room in the UNM IT datacenter that can be accessed through only one door using a badge system. Physical security controls are necessary to ensure unauthorized individuals do not obtain access to the datacenter.

UNM IT maintains two guest badges that must be checked out by vendors prior to accessing the datacenter. Although vendors must check out a badge and sign a sign-in sheet prior to accessing the datacenter, they are left unsupervised so they can leave and re-enter as they like.

Internal Audit reviewed the datacenter access logs from the badge system. The logs indicated that one vendor accessed the datacenter five times on 7/22/2015 and six times on 7/23/2015; another vendor accessed the datacenter two times on 6/30/2015, two times on 7/23/2015, four times on 8/4/2015, and nine times on 8/18/2015.

In addition, Physical Property Department employees have unsupervised access to the datacenter to perform maintenance.

Internal Audit reviewed datacenter access logs to determine if only authorized UNM employees and/or guests accessed the datacenter. Internal Audit noted a UNM employee identification number that accessed the datacenter one time and a visitor identification number that accessed the datacenter eleven times between 7/22/2015 and 7/23/2015. Neither of the identification numbers were on an authorized access listing. In addition, a University of New Mexico Hospital (UNMH) employee is on the authorized access listing, although UNMH does not have any servers in the datacenter.

Physical Security best practices suggest non-IT personnel, such as Physical Plant Department employees and vendors, be escorted to and from a restricted area and supervised while in the restricted area. Unsupervised access to the datacenter increases the risk of Banner data being compromised or destroyed. Lack of adequate and consistent security administration procedures may result in the unauthorized use, disclosure or modification, and damage or loss to systems or data.

Recommendation 8

Non-IT personnel and/or visitors that access the Banner datacenter should be supervised at all times or compensating controls should be developed to control the access of these individuals. In addition, accurate authorized access listings should be maintained and updated on a regular basis and user access should be reviewed on a regular basis.

Response from the Chief Information Officer

Action Items
Targeted Completion Date: *5/18/2016*
Assigned to: *Chief Information Officer*
Corrective Action Planned: *We concur. We have implemented the compensating controls of pre-authorizing, controlling access via a multi-factor ID card, logging, and recording the entrance via security camera of the Non-IT personnel who have a recurring and legitimate business need to access the Data Center. These authorized personnel are given training and access based on their job duties. We agree, and have put procedures in place, that all other visitors who do not have a regular business need to access the datacenter (including emergency responders) must be escorted at all times while in the Data Center. Additionally, we propose to install additional security cameras (approximately 11) inside the Data Center to monitor the servers and equipment as an additional compensating control. Video monitoring has been implemented at Texas Tech University and Temple University. We have also updated our Data Center Access Procedures to include the requirements to maintain and update authorized access listings, and to review user access on a regular basis.*

APPROVALS

Manu Patel, CPA
Director, Internal Audit Department

Approved for Publication

Chair, Audit and Compliance Committee