Banner Access
Registrar's Office

Audit Report # 17-06
August 21, 2017

The University of Texas at El Paso
Institutional Audit Office

"Committed to Service, Independence and Quality"

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

UTEP Institutional Audit Office
500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU
WWW.UTSYSTEM.EDU

August 21, 2017

Dr. Diana Natalicio
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited scope audit of Banner Access. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by Enterprise Computing and the Registrar's Office staff during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Mr. Richard Adauto III, Executive Vice President
Ms. Nohemi Gallarzo, Registrar, Registration & Records Office
Dr. Amanda Vasquez-Vicario, Assistant Vice President, Enrollment
Mr. Luis Hernandez, Director of Enterprise Computing
Dr. Stephen Riter, Vice President for Information Resources and Planning
Dr. Gary Edens, Vice President, Student Affairs
Ms. Sandy Vasquez, Assistant Vice President for Compliance Services

University of Texas System (UT System):
System Audit Office

External:
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office
Sunset Advisory Commission

Audit Committee Members:
Mr. David Lindau
Mr. Steele Jones
Mr. Fernando Ortega
Ms. Carol Parker
Mr. Benjamin Gonzalez
Dr. Roberto Osegueda

Auditors Assigned to the Audit:
Ms. Victoria Morrison, IT Auditor
Ms. Cecilia Estrada Lozoya, Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services (OACS) has completed an audit of the Banner Student Information System (SIS) Access. The audit scope was limited to grade change access, transcript access, and database access.

The source of the audit criteria is: The Texas Department of Information Resources (DIR), UTS165 Information Resources Use and Security Policy, and Family Educational Rights and Privacy Act (FERPA), 20 U.C.S. §1232 G.

During the audit we tested the following:

- compliance with applicable laws, regulations, and University policies and procedures for student records management,
- approval and authorization process for granting access to Banner SIS,
- access controls and monitoring of grade changes and transcripts, and
- safeguarding and integrity of student records.

The following are considered opportunities for improvement:

- Policies, procedures, and forms related to student records management need to be documented and up to date,
- a role-based access management system has not been developed,
- programmer access to grade changes is critical for the Registrar's Office operations; consequently, there is no separation of duties between enterprise system programmer(s) and the Registrar's business functions, and
- audit and review of restricted Oracle database privileges needs to be performed.

BACKGROUND

Banner Student Information System (SIS) Access was rated as high in the University-wide risk assessment by the Registrar.

The area of concern was access to transcripts and student grades changes. In question was the access granted by business requirements or needs. Another area of concern was access control to print unofficial transcripts, increasing the risk of exposing confidential student information.

The protection of student records is critical to comply with the Family Educational Rights and Privacy Act (FERPA), 20 U.C.S. §1232 G. This law provides students with rights with respect to their educational records. Therefore, unrestricted access to the Banner SIS and database create a risk for the University.

AUDIT OBJECTIVES

The objectives of this audit were to:

- Verify University compliance with applicable laws, regulations and University policies and procedures for student records management,
- ensure there is an approval and authorization process for Banner SIS,
- determine the level of staff training and awareness of federal and state regulations regarding student records,
- identify the type and effectiveness of controls over transcripts and grade changes, and
- ensure the safeguarding & integrity of student records on the Banner SIS.

SCOPE AND METHODOLOGY

The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors.

The audit addresses the high risk areas identified in the University-wide risk assessments for Fiscal Years 2016 and 2017.

The audit criteria includes:

- The Family Educational Rights and Privacy Act (FERPA), 20 U.C.S. §1232 G
- The Texas Public Information Act, Texas Government Code § 552.001 et seq;
- Texas Information Resource Department, Security Catalog (TAC 202.76.2)
- UTS165 Information Resources Use and Security Policy

The audit scope is limited to access control of the business application Banner SIS, including database access, beginning 09/01/2016 through 03/31/2017.

Audit procedures included:

- interviewing key personnel,
- reviewing applicable laws, regulations, policies and procedures,
- verifying the existence of appropriate institutional policies and procedures,
- requesting information from key personnel,
- question and answer, and
- limited testing where appropriate.

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority - 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.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

AUDIT RESULTS

1. Governance, Laws, Regulations, Policies and Procedures.

Requirements/Controls:

Texas DIR Security Control Standards Catalog:

AC-1 Access Control Policy;

AC-2 Account Management

AC-24 Access Control Decisions

UTS165 Sec. 15 Management of Sensitive Digital Data

UTS165 Standard Access Management

Observations:

Auditors received evidence of monitoring and review of Banner access by data owner. However, the process is not documented. The Registrar's Office and Enterprise Computing department have some written policies and procedures for access control, monitoring, and awareness. Additional policies should be documented for all monitoring and access procedures.

Lack of documented departmental policies and procedures can create confusion, decrease efficiency, and create a risk of possible FERPA violations or inappropriate access.

Recommendation:

A review of documented policies, procedures and forms should be performed at least every two years. Enterprise Computing and the Registrar's Office should work together to document:

- *the process flow for granting Banner SIS access,*
- *monitoring and review of Banner SIS access, and*
- *role-based Banner SIS access based on business requirements and any exceptions to the access.*

Level: This finding is considered **Medium**, due to undocumented controls. Therefore, operations are dependent on the knowledge and motivation of individuals.

Management Response:

While we were presented with one form that had outdated information, there was not additional information regarding incomplete or non-existent forms. Further, it is not accurate to note that there is an absence of departmental policies and procedures. There is already a process in place for monitoring and reviewing access to Banner. However, Enterprise Computing will work with Enrollment Services on developing a more role-based process for access and adjust processes accordingly.

Responsible Party:

Luis Hernandez, Edgar Luna

Implementation Date:

September 1, 2018

2. Access Controls and Monitoring Of Grade Changes

Requirements/Controls

Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C

- Rule 202.72 Staff Responsibilities
- Rule 202.76 Texas DIR Security Control Standards Catalog
  - AC-5 Separation of Duties
  - AC-6 Least Privilege
  - AC-2 Account Management
  - AC-21 Information Sharing

Observations:

Enterprise system programmer(s) perform the grade roll into production (post grades), and it is crucial for them to have update access to change grades in Banner SIS. The process occurs every other week during the year, so access cannot be removed and reinstated after grade roll process.

Separation of duties between enterprise system programmer(s) and registrar business functions needs to exist. Separation of duties reduces the risk of conflict of interest, as well as the appearance of conflict of interest, along with errors or unapproved changes.

The total number of users with approved access is 18 users: 11 from the Registrar and 7 from other departments.

Recommendation:

Implement mitigating controls to remediate enterprise system programmers' update access to production. Develop and document a monitoring and review process for unapproved grade changes.

Level: This finding is considered **Medium,** due to lack of segregation of duties, which may result in unauthorized or unintentional modification or misuse of the organization's information assets.

Management Response:

There is a concern with the notation that there is not a separation of duties between Enterprise System Programmers and the Registrar's staff, as that suggestion is too far-reaching and does not adequately acknowledge that in truth there is separation of duties between the two offices. However, we do acknowledge that the level of system access is the same for the two groups. The Enterprise Computing programming team requires the access listed above to complete the grade roll process. Enterprise Computing will work with Enrollment Services to implement controls to mitigate the risk of unauthorized changes, but due to staffing limitations they will continue to require that level of access in order to complete their assigned responsibilities. The only alternative would be to hire a programmer to work in Enrollment Services to fill that requirement and that is just not a viable solution.

Responsible Party:

Luis Hernandez, Edgar Luna, and Amanda Vasquez

Implementation Date:

December 1, 2017

3. Job Function-Access Control

Requirements/Controls

Texas Administrative Code Title 1, Part 10, Chapter 202, SubChapter C

- Rule 202.72 Staff Responsibilities
- Rule 202.76 Texas DIR Security Control Standards Catalog
  - AC-2 Account Management
  - AC-3 Access Enforcement
  - AC-6 Least Privilege
  - AC-21 Information Sharing
  - IA-1 Identification and Authentication Policy and Procedures

UT System Information Resources Use and Security Policy 165

UTS165 Standard 4: Access Management, 4.5 Data Access Control Requirement.

Observations:

Although Enterprise Computing has established the access classes, a defined structure with roles (job function) and access assigned to each role has not been developed.

As there is no structure with set roles and access level associated with it, each request is evaluated individually to determine which level of access and read/write privileges should be granted. Therefore, the risk increases if the application is accessed by users outside of defined business functions.

Recommendation:

Enterprise Computing and the Registrar's Office should work together to develop and document a role-based access control that is limited to the business functions. Additionally, any exceptions that do not follow the access control should be documented.

Level: This finding is considered **Medium,** due to misconfigured access controls which may provide unauthorized access to information in application systems.

Management Response:

Enterprise Computing will work with Enrollment Services on developing a more role-based process for access, keeping in mind that the business requirements may create situations where the exceptions become the rule.

Responsible Party:

Luis Hernandez and Edgar Luna

Implementation Date:

September 1, 2018

4. Restrict and Define Database Privileges

Requirements/Controls

Texas Administrative Code Title 1, Part 10, Chapter 202, SubChapter C

Rule 202.72 Staff Responsibilities

Rule 202.76 Texas DIR Security Control Standards Catalog

AC-5 Separation of Duties

AC-6 Least Privilege

AC-2 Account Management

AC-3 Access Enforcement

CM-6 Configuration Setting

Observations:

Overall, the safeguarding & integrity of student records were in place with the following exceptions:

- Two database roles with access to modify production tables were granted to non-database administrators (DBA),
- the Enterprise Computing department has no documented separation of duties matrix to define the tasks and the type of database access based on job function in order to prevent inappropriate access, and
- someone other than the DBA has the ability to grant roles to other database accounts.

These exceptions could lead to inappropriate access, incorrect assignments to unauthorized accounts, and/or unapproved changes.

Recommendation:

Enterprise Computing should audit and review database access after any personnel changes to ensure the appropriate access or privileges are in place for all database accounts. Create a documented separation of duties matrix to define tasks and the type of database access based on job function. Document the results as well as any exceptions to the database access structure.

Level: This finding is considered **Medium,** due to possible inappropriate database access controls which could result in unauthorized access or privileges.

Management Response:

Access is reviewed upon personnel changes or changes in job requirements. Staffing requirements make it necessary to grant that level of access to the programming team in order for the work to be completed. However, we do acknowledge that the level of system access is the same for the two groups and as a result, Enterprise Computing will work with Enrollment Services to implement controls to mitigate the risk of unauthorized changes and document the separation of duties.

Responsible Party:

Luis Hernandez, Edgar Luna and Amanda Vasquez

Implementation Date:

December 31, 2017

5. Additional Audit Procedures Areas

5.1. Approval and authorization process for Banner SIS

An approval process for granting Banner SIS access is initiated by entering a Help Desk ticket. The documents related to the access approval of a specific account are contained within the service desk ticket.

The process appeared appropriate and includes an audit trail via the Help Desk ticket.

No exceptions were noted.

5.2. Compliance and awareness training for federal and state regulations regarding student records

Users with Banner SIS accounts receive mandated yearly compliance training provided by the Office of Institutional Compliance. A new Banner SIS user will receive their account only after they complete the "Banner Introduction Training".

Adequate identification is required to receive transcripts. This information is clearly posted at the Registration and Records Office.

No exceptions were noted.

5.3. Access controls and monitoring of transcripts

In December 2016 there were 222 users with the ability to print non-official transcripts. During the audit the amount decreased to 132 users. Official transcripts are processed through an outside vendor. Undergraduates and work studies have access to print transcripts if their job/business function is undergraduate advisors.

No exceptions were noted.

CONCLUSION

Audit results show opportunities for improvement in control processes which we believe can be strengthened by implementing the recommendations detailed in this report.

We wish to thank the management and staff of the Registrar's Office and Enterprise Computing for their assistance and cooperation provided throughout the audit.

CRITERIA

Texas Administrative Code Title 1, Part 10, Chapter 202, SubChapter C
Rule 202.72 Staff Responsibilities

Information owners, custodians, and users of information resources shall, in consultation with the institution IRM and ISO, be identified, and their responsibilities defined and documented by the state institution of higher education. The following distinctions among owner, custodian, and user responsibilities should guide determination of these roles:
(1) Information Owner Responsibilities. The owner or his or her designated representative(s) are responsible
for:
(A) classifying information under their authority, with the concurrence of the state institution of higher education head or his or her designated representative(s), in accordance with institution of higher education's established information classification categories;
(B) approving access to information resources and periodically review access lists based on documented risk management decisions;
(C) formally assigning custody of information or an information resource;
(D) coordinating data security control requirements with the ISO;
(E) conveying data security control requirements to custodians;
(F) providing authority to custodians to implement security controls and procedures;
(G) justifying, documenting, and being accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the institution of higher education information security officer; and
(H) participating in risk assessments as provided under §202.75 of this chapter.
(2) Information Custodian Responsibilities. Custodians of information resources, including third party entities providing outsourced information resources services to state institutions of higher education shall:
(A) implement controls required to protect information and information resources required by this chapter based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the institution of higher education information security program; (B) provide owners with information to evaluate the cost effectiveness of controls and monitoring;
(C) adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents;
(D) provide information necessary to provide appropriate information security training to
(E) ensure information is recoverable in accordance with risk management decisions.

...

Texas Department of Information Resource-Security Control Standards Catalog (TAC 202-76)

AC-1 Access Control Policy and Procedures

...

Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
Procedures to facilitate the implementation of the access control policy and associated access controls; and
Reviews and updates the current:
Access control policy [Assignment: organization-defined frequency]; and
2. Access control procedures [Assignment: organization-defined frequency].

...

Each state organization shall create, distribute, and implement an account management policy which defines the rules for establishing user identity, administering user accounts, and establishing and monitoring user access to information resources

...

AC-2 Account Management

...

c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
g. Monitors the use of, information system accounts;
h. Notifies account managers:
1. When accounts are no longer required;
2. When users are terminated or transferred; and
3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements [Assignment: organization- defined frequency]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety. Information resources assigned from one state organization to another or from a state organization to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing state organization.

...

AC-3 Access Enforcement

...
1. Access to state information resources shall be appropriately managed.
2. Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.

...
Example:
The organization has implemented role-based access control to determine how users may have access strictly to those functions that are described in job responsibilities.

...

AC-5 Separation of Duties

...
Separates [Assignment: organization-defined duties of individuals];
Documents separation of duties of individuals; and
Defines information system access authorizations to support separation of duties.

..
State organizations shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

...

AC-6 Least Privilege

...
Control Description: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

...

AC-21 Information Sharing

...
Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and
Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

...
User login credentials are provided based on job responsibilities and periodically reviewed for appropriateness

...

AC-24 Access Control Decisions

...
The organization establishes procedures to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.

...

CM-6 Configuration Settings

...

Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

...

IA-1 Identification and Authentication Policy and Procedures

...

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Reviews and updates the current:
1. Identification and authentication policy [Assignment: organization-defined frequency]; and
2. Identification and authentication procedures [Assignment: organization-defined frequency].
IMPLEMENTATION

The state organization establishes the policies for verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in an information system

...

UTS165 Information Resources Use and Security Policy

UTS165 Sec. 15 Management of Sensitive Digital Data

15.1 Protection. Each Entity's policies, standards, and/or procedures must describe and require appropriate steps to protect Sensitive Digital Data (e.g., social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law) stored on U. T. System's computing devices.
15.2 Access. All Entities shall control and monitor access to their Sensitive Digital Data based on Data sensitivity and risk (as determined in accordance with Section 14 of this Policy) and by the use of appropriate physical and technical safeguards.
(a) All Entities shall limit access to records containing Sensitive Digital Data to those employees who need access to the Data for the performance of the employees' job responsibilities.

...

(b) All Entities shall monitor access to records containing Sensitive Digital Data by the use of appropriate measures as reasonably determined by the Entity.

...

UTS165 Standard 4: Access Management

...

4.2 Access Management Process : An Access Management Process must incorporate Procedures for:

...

(b) creating uniquely identifiable accounts for all Users. This includes accounts created for use by Vendors (see Standard 22);
(c) disabling all generic and default accounts;
(d) reviewing, removing and/or disabling accounts at least quarterly, or more often if warranted by Risk, to reflect current User needs or changes of User role or employment status;
(e) expiring Passwords or disabling accounts based on Risk; and

...

4.5 Data Access Control Requirement. All Owners and Custodians must control and monitor access to Data within their scope of responsibility based on Data sensitivity and Risk, and through use of appropriate administrative, physical, and technical safeguards including the following:
(a) Owners must limit access to records containing Confidential Data to those employees who need access for the performance of the employees' job responsibilities. An employee may not access Confidential Data if it is not necessary and relevant to the employee's job function.
(b) Owners and Custodians must monitor access to records containing Confidential Data by the use of appropriate measures as determined by applicable Policies, Standards, Procedures, and regulatory requirements.
(c) Owners and Custodians must establish log capture and review processes based on Risk and applicable Policies, Standards, Procedures, and regulatory requirements. Such processes must define:
1. the Data elements to be captured in logs;
2. the time interval for custodial review of the logs; and
3. the appropriate retention period for logs.

...

GLOSSARY

Term	Definition
Job Function/Business Functions	The routine set of tasks or activities undertaken by a person in that job position. An employee's title and function are often closely related, though not all job functions are clear based on title alone or job description. Access is related to job function not necessarily job title.
Job Title	Position name given in People Soft
Peer Advisor	Serve as members of the Undergraduate Advising Center (UAC) staff and assist students as they experience a variety of transitions including acclimation to academic life, major selection and overall academic success.
Separation of Duties(SoD)	One of the key concepts in placing internal controls over a company's assets is segregation of duties. Segregation of duties serves two key purposes: It ensures that there is oversight and review to catch errors. It helps to prevent fraud or theft because it requires two people to collude in order to hide a transaction
Mitigation	A mitigating control is type of control used in auditing to discover and prevent risks that may lead to uncorrected and/or unrecorded misstatements that would generally be related to control deficiencies