




BANNER – Student Records System Internal Audit Report
Project # 2017-31
October 25, 2017

Reviewed by:


Taylor Eighmy, Ph.D.
President

Executive Summary
BANNER – Student Records System Internal Audit Report
Project # 2017-31

Objectives:

Review the operational efficiency and the effectiveness of the application controls of the Student Records Information System (BANNER).

Scope:

The current BANNER OIT development staff and user community are fully engaged in the project to move the system to the new hosting environment and upgrade to version 9. Both of these items will have a significant impact on the functionality of the system, as well as, how it is administered and supported. Due to these fundamental changes within the control environment of BANNER, the application controls were not reviewed. As a part of our annual risk assessment, we will determine if an audit of the specific application controls within this new environment is warranted for next year. However, through interviews and limited testing during the planning phase of the audit, three strategic governance and management observations were identified.

Conclusion:

Strategic data governance and automated data integrity controls need improvement. UTSA's data analytics and reporting requirements have significantly changed and increased since the initial implementation of the BANNER system in 2002. Moreover, with increased regulations and funding challenges, these requirements have become exponentially more complex within the past 10 years. UTSA's data collection, management processes and automated controls have not evolved to efficiently and effectively collect and ensure the integrity of the data being analyzed and reported.

Non-Priority Recommendations:

- Implement strategic data governance processes. (High)
- Improve automated transaction and data logging. (Medium)
- Resolved basic segregation of duties concerns between IT development, user responsibilities, and security administration. (High)

A Priority Finding is defined as *“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.”* Non-Priority Findings are ranked as High, Medium, or Low, with the level of significance based on an assessment of applicable Qualitative, Operational Control, and Quantitative risk factors and probability of a negative outcome occurring if the risk is not adequately mitigated. This audit resulted in two High and one Medium-level findings, but no Priority Findings.

Audit Results
BANNER – Student Records System Internal Audit Report
Project # 2017-31

Background

UTSA utilizes Ellucian's Banner Student Software Suite integrated with other Ellucian software offerings for student administration (BANNER). UTSA's BANNER system utilizes the following Ellucian software modules:

- Student (version 8.9) - Comprehensive student strategic management and records processing.
- Accounts Receivable (version 8.5) - Subset of the Banner administrative system. Used to maintain charge and payment information for individual accounts
- BDMS (version 8.5) – Database that provides a data bridge between Banner and Xtender, the Ellucian document imaging product.
- Financial Aid (version 8.2.9) – Disburse and monitor funds.
- General (version 8.8.1) – Core BANNER system component.
- Integration Components (version 8.0.2) – Component that allows integration with other Ellucian and non-Ellucian systems such as eLearning, Degree Works, Xtender document imaging, Recruiter, CourseLeaf and others.
- Web General (version 8.7.1) – Module for student, faculty and staff Self-Service (ASAP)
- Banner Self Service Modules (ASAP):
 - Web Tailor (version 8.7) – The configuration component
 - Faculty & Advisor SS (version 8.7) – Allows faculty members and advisors to access class information and enter grades.
 - Financial Aid SS (version 8.2.5) – Automated, online checklist that keeps everyone on track and up to speed when navigating the financial aid process.
 - Student SS (version 8.7) – Lets students conduct their business online, from buying books to registering for course to getting financial aid.

The implementation and integration of these modules supports a full range of academic administration functions including but not limited to: class scheduling, admissions, registration, accounts receivable, financial aid process, transcript management, faculty workload analysis, academic history and degree audit reporting, census and other government reporting.

Audit Details

Review the operational efficiency and the effectiveness of the application controls of the Student Records Information System (BANNER).

Data Integrity

The Mission Statement of The Office of the Registrar is to provide high-quality service, **accurate student records management**, and timely reporting of enrollment information

Audit Results

BANNER – Student Records System Internal Audit Report Project # 2017-31

utilizing leading-edge technology to the multi-campus university community.

Data integrity is the maintenance of and the assurance of the accuracy and consistency of data over its entire life cycle (origination to destruction). How the data is entered, processed, stored and managed has a direct effect on data integrity and quality. The dimensions of data quality include:

- Accuracy - Does the recorded data match the original source?
- Timeliness – How much time does it take to record the data?
- Completeness – How much of the stored data is 100% complete?
- Validity – Does the recorded data conform to the business rules definition?
- Uniqueness – Are there duplicate records for the same thing or person?
- Consistency - Are there differences when comparing across data systems?

Data Governance is an institutional strategy employed to ensure foundational data is robust and trustworthy to meet processing, reporting and management needs. Data governance focuses on improving data quality and accuracy, protecting access to data, establishing business definitions, maintaining metadata and documenting data policies. Data governance formalizes processes about how data is defined, produced, used, and stored in order to enable and enhance organizational effectiveness.

Observation:	Data fields within BANNER contain inaccurate data that has a wide range effect on the admissions, registration, financial aid processes and the ability to produce timely accurate governmental and data analytical reports. Furthermore, there is a lack of a data governance structure to facilitate the correction of the data and proactively establish controls to ensure data integrity within the system. Substantial data characteristic and processing decisions are made in departmental silos without a full understanding of the downstream or cross process, affect or consideration for needed integrity controls. Integrity controls, such as edit/validation checks and automated approvals have been limited due to the fear of slowing down the systems
---------------------	---

Audit Results
 BANNER – Student Records System Internal Audit Report
 Project # 2017-31

	response/processing time and lack of hardware processing capacity.
Risk Level:	The risk of incorrect data entries and siloed activities regarding data governance is considered High due to the impact incomplete or inaccurate data can have on student eligibility, reporting and strategic endeavors.
Management's Response:	A task force will be formed to perform a comprehensive review to evaluate the data governance and integrity discrepancies within BANNER. Processes within each area supporting and utilizing the data will be evaluated to determine where we can automate entries to avoid human mistakes. A review of Banner access classes will be performed and adjustments will be made based on new federal guidelines as well as assigning appropriate update access to Banner across campus. BANNER version 9 features will be reviewed to determine if they can be utilized to improve data integrity. A plan with recommendations for changes within BANNER and across all departments affected will be outlined with proposed implementation tasks and dates.
Responsible Person:	Sr. AVP for Student Affairs
Implementation Date:	Task Force Launch Date: January 2018 Plan Completion Date: August 31, 2018 Implementation Date: TBD by plan

Transaction History Logs

In an application, a transaction log or audit trail is a history of actions executed or data changed in the application and/or database. It is a chronological set of records and relevant information regarding source and destination that provide documentary evidence of the sequence of activities that have affected at any time a specific data field, operation, procedure, or event. Transaction logs/audit trails provide the operational users with the flow of transactions or changes through a system allowing for the detections, alerting, and correction of unexpected or inappropriate changes. To be able to investigate which user or process accessed or changed the data, the information must be logged.

The data maintained in BANNER is critical to several institutional operations. Entering, storing, and maintaining valid data in the database is the most important job function of this application. When multiple users/departments/process can change the data, the institution should maintain transaction logs or audit trails of data changes to critical attributes and student

Audit Results

BANNER – Student Records System Internal Audit Report Project # 2017-31

data to track who made the changes to the data. Tracking changes has two benefits:

- it can be determine which users are consistently making mistakes (or not making mistakes).
- mistakes can be undone before queries and reports start producing erroneous data or processes start malfunctioning.

Having a detailed transaction log or audit trail can protect the institution from liability during legal inquiries, help monitor data for security breaches, ensure proper protocols are followed and demonstrate compliance. It can also be used to strengthen your team and operations by identifying training opportunities and operational process changes to increase efficiency and effectiveness.

Observation:	Current transaction and data change logging is limited within BANNER. Due to the concerns that any logging will affect the applications performance and response time, this practice has been avoided by UTSA. OIT recommends that if users want faster response they should limit the number of logs used within the system. Limited testing of different logging has been performed throughout the years since BANNER was implemented.
Risk Level:	The risk of not logging activity on Banner Forms where critical data and configuration parameters are changed is considered Medium due to the inability to consistently establish, correlate, investigate, or identify responsible parties should an inappropriate change or event occur. While compensating manual quality control efforts are in place for some forms, automated processes could be more accurate and efficient in tracking changes to critical data and configuration components.
Management's Response:	Several forms in banner are already set up to log when changes are made to student accounts and in some cases, overarching forms that are used for setting up award/aid years. Based on the observations stated above, we will do a comprehensive review of the forms that are currently set up for logging and review all of the Banner forms that have a significant impact on eligibility, status, etc. and make a determination to track changes via logging of User IDs. If the form allows for logging, we will make changes as appropriate. If the Banner form does not have a logging feature then we will determine if additional measures need to be in place to mitigate the risk in other ways via quality control or report generation.

Audit Results
 BANNER – Student Records System Internal Audit Report
 Project # 2017-31

Responsible Person:	Sr. AVP for Student Affairs
Implementation Date:	August 31, 2018

Separation of Duties

Separation of Duties (SoD) is a basic building block of sustainable risk management and internal controls for a business. The principle of SoD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. The separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud, error and single points of failure within a process. As a best practice for UTSA, the person(s) responsible for critical information security duties should be separated from the rest of the IT operational duties and functions.

The most basic separations is between the Information Technology (IT), Information Security (IS), and user department functions. While a user department will occasionally have separate groups that provide help desk, business/system analysts, report writing, or application security administration, it should not do its own programming and other critical IT or IS duties. The IT teams should also not assume critical user roles and IS application security administration.

User departments should be expected to provide input into systems and application development (i.e., information requirements) and provide a quality assurance function during the testing phase. A common principle of application development is to ask the users of an application to test it before it goes into operation. Then, the user department would sign a user acceptance agreement to indicate it is performing according to the information requirements. Additionally, IT should not have the ability to give themselves access to production data/systems as this can compromise established data integrity and application change management controls.

Observation:	<p>IA identified three basic (Separation of Duties) SoD issues within the BANNER administration structure:</p> <ol style="list-style-type: none"> 1. The user departments currently employ application development programmers who are utilized to write add-
---------------------	--

Audit Results

BANNER – Student Records System Internal Audit Report Project # 2017-31

	<p>on/sub-applications to BANNER (i.e. Orientation) and modify BANNER application scripts and packages, which affect the core application processing and update data tables.</p> <ol style="list-style-type: none"> 2. The OIT application team currently manages the roles and role assignments which provide access to the BANNER web front end portion of the application (specifically called ASAP or technically labeled by vendor as Web Tailor) 3. The BANNER Security Administration Team reports to the User Application Development Team. It is our understanding this SoD has recently been resolved.
<p>Risk Level:</p>	<p>To mix critical IT, IS and user departments duties is to increase risk associated with errors, fraud and sabotage. The lack of basic segregation of duties in Banner IT functions is considered High risk as that alignment of people, process and technology is not effectively creating awareness of inefficiencies and increased risks that potentially affect system availability and achievement of business objectives.</p>
<p>Management's Response:</p>	<ol style="list-style-type: none"> 1. The President has created a new Strategic Enrollment Planning task force, which will include a review of processes and organizational structure to ensure we are meeting our enrollment objectives. Many institutions across the country have enrollment management divisions or structures that also include technical staff that serve as developers for their Student Information Systems. In light of the concerns about risks to Banner processes and applications and the fact that we are taking a comprehensive look at our strategic enrollment efforts, we will evaluate the current structure and make recommendations for potential changes as they fit into the strategic enrollment efforts of the university. Until those recommendations are available, we will enhance testing processes to ensure any changes made within the departments are fully vetted before moving into production. Note that developers in the departments do not make changes to Baseline Banner. Enrollment Services has an individual who works in ADS (funded by Enrollment Services). That individual can make changes to baseline banner under the supervision of ADS.

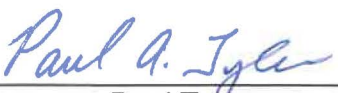
Audit Results
BANNER – Student Records System Internal Audit Report
Project # 2017-31

	<p>2. In reference to the OIT application team managing the roles and role assignments for access to the Banner web front-end portion of the application (ASAP), we will change that process and move it to the Banner Security Team.</p> <p>3. As of November 2, 2017, The Banner Security Team will report directly to the Sr. Associate VP for Student Affairs and not to a User Application Development Team. Additionally, A review of Banner access profiles will be reviewed this year and adjustments will be made per new federal guidelines for financial aid and to ensure access is appropriate across the campus.</p>
Responsible Person:	Sr. AVP for Student Affairs
Implementation Date:	August 31, 2018


CONCLUSION

Strategic data governance and automated data integrity controls need improvement. UTSA's data analytics and reporting requirements have significantly changed and increased since the initial implementation of the BANNER system in 2002. Moreover, with increased regulations and funding challenges, these requirements have become exponentially more complex within the past 10 years. UTSA's data collection, management processes and automated controls have not evolved to efficiently and effectively collect and ensure the integrity of the data being analyzed and reported.

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



 Paul Tyler
 Interim Chief Audit Executive



 Carol Rapps
 Audit Manager, Information Systems