AUDIT OF INTERNET NATIVE BANNER APPLICATION SECURITY

UNIVERSITY OF NEW MEXICO

Report 2007-10
September 22, 2008

Audit Committee Members

J.E. "Gene" Gallegos, Chair
Lt. Gen. Bradley Hosmer, Vice Chair
James Koch

Audit Staff

Manu Patel, Audit Director
Yvonne Cox, Internal Audit Manager
Lisa Wauneka, Information Systems Auditor
Richard Swanson, Senior Auditor

CONTENTS

ABBREVIATIONS

Banner	Internet Native Banner
COBIT	Control Objectives for Information and related Technology
ERP	Enterprise Resources Planning
Oracle	Oracle Relational Database Management System
UBP	University Business Policies and Procedures Manual
University	The University of New Mexico
UNM	The University of New Mexico

EXECUTIVE SUMMARY

The Internal Audit Department 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, a product of SunGuard Higher Education, 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.

University management should develop a formal security infrastructure to ensure that there are adequate and effective information system controls for Banner. This will ensure that the Banner information system functions as intended and protects the sensitive information processed and stored by Banner.

BANNER SECURITY PLANNING AND ORGANIZATION

University management should develop a formal governance and organizational structure for Banner security. Management should designate a centralized security function with adequate staffing to administer Banner security from a global perspective. Internal Audit addressed recommendations in this report to University management because the University does not have clearly defined responsibilities and authority for security administration. University management should develop and enforce Banner security policies and require the Enterprise Resources Planning (ERP) Steering Committee [1]to develop a charter. The Chief Information Officer, the Provost and Executive Vice President for Academic Affairs, and the Executive Vice President for Administration will develop a governance and organization structure, review staffing, and define roles and responsibilities for security administration of Banner.

UNIVERSITY BUSINESS POLICIES

The Executive Vice President for Administration should develop a policy addressing the process of adding and maintaining policies. The Director of Information Assurance should develop a remote access policy addressing access into University information systems.

BANNER APPLICATION AND ORACLE DATABASE SECURITY

University management should develop Banner and Oracle relational database management system (Oracle) security administration documentation. The Chief Information Officer, the Provost and Executive Vice President for Academic Affairs, and the Executive Vice President for Administration stated that the Chief Information Officer will lead the development of Banner and Oracle security administration documentation.

[1] The ERP Steering Committee is accountable to deliver increasing value to the University community through the deliberate and effective administration of UNM's mission critical student, research and administration functions. The ERP Steering Committee makes decisions related to ERP policy, process and investment, prioritizing those efforts which have the greatest impact on University success.

INTRODUCTION

BACKGROUND

Banner, an integrated suite of administrative applications, is the core administrative system at the University that gives users access to perform their job duties. Consisting of the Banner modules for Finance, Student, Financial Aid, General, Budget Development, and Human Resources, 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 and the Oracle require proper administration and security to protect the systems and data. Banner security is administered primarily by ERP Data Security Specialists.

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 ensure the information system functions as intended and to protect the sensitive information processed and stored by Banner.

PURPOSE

The audit purpose is to ensure the University has developed an adequate and effective system of information system controls for Banner and the Oracle relational database management systems. These controls should include the following:

- Effectiveness and efficiency of operations.
- Reliability of information.
- Compliance with laws and regulations.
- Confidentiality, integrity, and availability of Banner information systems and data.

SCOPE

The Internal Audit Department conducted an audit of selected general and application system controls relating to the Internet Native Banner application and the Oracle relational database management system.

The audit scope consisted only of Internet Native Banner and included the following:

- Review of applicable University information system policies and procedures.
- Review of Internet Native Banner-related security policies and procedures.
- Review of the security administration for Internet Native Banner.
- Review of the security administration for Oracle.

The audit consisted of interviews, reviews of documentation, and a statistical sample of Internet Native Banner Oracle users. Audit fieldwork was completed in March 2008. We developed Audit criteria using the following sources.

- Control Objectives for Information and related Technology (COBIT). COBIT’s purpose is to develop and publish best practices for Information Technology Governance.
- Oracle Database Security, Audit and Control Features.
- Oracle Security Step-by-Step.
- Banner Technical Reference Manual.

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

BANNER SECURITY PLANNING AND ORGANIZATION

The University has not formally defined and adopted Banner security procedures and responsibilities. Because the University has devoted resources to Banner implementation, resources have not been available for developing Banner security.

Formal Governance and Organizational Structure and Centralized Security Structure

The University has not established a formal governance and organizational structure to administer Banner security or assigned information system security responsibility to a centralized security organization with a global security perspective.

Recommendation 1

The Chief Information Officer, the Provost and Executive Vice President for Academic Affairs, and the Executive Vice President for Administration should:

- Develop a formal governance and organizational structure for Banner security.
- Assign Banner security administration functions to a centralized security administration organization.

Response from the Chief Information Officer, the Provost and Executive Vice President for Academic Affairs, and the Executive Vice President for Administration

On or before April 17, 2009, the Chief Information Officer, in conjunction with the Provost and the EVP for Administration,

a) *Will review the existing Banner security organizational structure,*

b) *Accept recommendations from the ERP Leadership Committee, the ERP Steering Committee, the Banner development & support teams, and the Information Assurance team on how best to organize and address Banner security,*

c) *Decide on an appropriate organizational structure, staffing level and budget to address findings # 1 and #3, and then*

d) *Work with the Provost and the EVP for Administration to address any resulting staffing and funding issues.*

ERP Steering Committee Charter

The ERP Steering Committee is the appropriate umbrella committee for Banner planning and coordination. The ERP Steering Committee has not developed a charter detailing the committee's responsibilities; therefore, it is unclear if Banner security planning falls under the purview of this committee.

Recommendation 2

The ERP Steering Committee should develop a charter detailing the committee's responsibilities.

Response from the Chief Information Officer, the Provost and Executive Vice President for Academic Affairs, and the Executive Vice President for Administration

On or before January 16, 2009, the Chief Information Officer will work with both the ERP Leadership and ERP Steering Committees to develop formal governance documents including mission statements and charters for both teams.

UNIVERSITY BUSINESS POLICIES

Remote Access Policies

The University has not developed remote access policies and procedures for access into the University information systems.

User authentication policies should include policies on remote access. Other universities have developed policies and procedures for remote access to information systems.

Prior to January 2008, when the Director of Information Assurance was hired, the University did not have a position assigned to develop information security policies.

Recommendation 3

The Director of Information Assurance should develop a remote access policy for University information systems.

Response from the Director of Information Assurance

On or before January 30, 2009, the Manager of the UNM Policy Office in conjunction with the Director for Information Assurance, IT Cabinet, the IT Managers Council, and the IT Agent Networking Group, will develop and present a University Business Policy on “Remote Access to University Information Systems” to the President for his consideration.

University Business Policies and Procedures Manual (UBP) Policy Updates for the Banner System

The University has not updated the following UBP policies with information on the Banner system.

1. "Computer Security Controls and Guidelines" Policy 2520, UBP.

    - The last update was July 2001 and the policy does not contain references to the Banner system.
    - The policy does not reflect a name change from the department of Computer and Information Resources and Technology to Information Technology Services.
    - Section 2.1.3. Access to University Information refers to the data custodians or owners of CIRT maintained systems. The owners and the systems listed have not been revised for the Banner system. System owners of Banner modules need to be assigned and documented.

2. "Access to Administrative Computer Systems" Policy 2590, UBP.

    - The last update was July 2004.
    - Section 3. System and Data Custodians contains a broken link to the system administrator web page.
    - Section 4. User Access process described in the policy is outdated. The policy needs to be revised for the current process.

The UBP Manual preface states "The UBP Manual is published by the University of New Mexico Policy Office and has been constructed in a format that is easily updated, added to, or otherwise modified. Each departmental executive is responsible for ensuring the Manual assigned to the department is kept current."

UBP policies do not state the job title of the departmental executive responsible for each policy. University policies related to information security should be adequate and maintained. Policies may not provide adequate guidance to users if they are not updated on a timely basis.

Recommendation 4

The Manager of the UNM Policy Office and the Chief Information Officer should update the following policies to reflect changes that occurred due to the implementation of Banner:

- "Computer Security Controls and Guidelines" Policy 2520, UBP.
- "Access to Administrative Computer Systems" Policy 2590, UBP.

Response from the Manager of the UNM Policy Office and the Chief Information Officer

On or before February 27, 2009, the Manager of the UNM Policy Office in conjunction with the Director for Information Assurance, the IT Cabinet, the IT Managers Council, and the IT Agent Networking Group, will develop and present updates to University Business Policies 2520 ("Computer Security Controls and Guidelines") and 2590 ("Access to Administrative Computer Systems").

Recommendation 5

The UNM Policy Office should develop a UBP Policy detailing how policies are developed and maintained. Policy maintenance should include a process to periodically review existing policies. This policy should designate by job title the departmental executive responsible for ensuring policies are reviewed and updated with the UNM Policy Office on a regular basis.

Response from the Executive Vice President for Administration

On or before March 1, 2009, the Manager of the UNM Policy Office, in conjunction with all concerned constituencies, will develop a Policy on Policies that defines development, revision, and communications protocols including review, endorsement, and approval requirements and present it to the President for his consideration.

BANNER APPLICATION AND ORACLE DATABASE SECURITY

As part of the audit scope, Internal Audit reviewed the administration of security for Internet Native Banner and the Oracle relational database management system. The implementation of Banner modules has consumed University resources for several years; however, the University did not dedicate adequate resources to implement Banner security and to develop the appropriate infrastructure, policies, procedures, and standards for Banner security. The following issues related to Banner security administration are a result of the lack of resources dedicated to Banner security.

Banner and Oracle Security Administration Procedures Manual

Security administration policies and procedures, including roles and responsibilities relating to Banner and the Oracle database have been developed but are incomplete. This lack of adequate and consistent security administration procedures may result in the unauthorized use, disclosure or modification, damage or loss to systems or data.

Recommendation 6

Security administration policies and procedures, including roles and responsibilities relating to Banner and the Oracle database should be updated and completed.

Response from the Chief Information Officer, the Provost and Executive Vice President for Academic Affairs, and the Executive Vice President for Administration

Security administration policies and procedures will be updated and completed by October 2009.

CONCLUSION

University management needs to develop a formal security infrastructure with adequate and effective information system controls for Banner. This will ensure that the Banner information system functions as intended and protects the sensitive information processed and stored by Banner.

APPROVALS

Manu Patel

Manu Patel
Director, Internal Audit Department

Approved for Publication

Chair, Audit Committee