A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

University of Arizona

Year Ended June 30, 2007

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

The **Auditor General** is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits of school districts, state agencies, and the programs they administer.

Copies of the Auditor General's reports are free.
You may request them by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Additionally, many of our reports can be found in electronic format at:
www.azauditor.gov

University of Arizona
Report on Internal Control and Compliance
Year Ended June 30, 2007

Table of Contents Page

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

Independent Auditors' Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

The Arizona Board of Regents

We have audited the financial statements of the business-type activities and aggregate discretely presented component units of the University of Arizona as of and for the year ended June 30, 2007, which collectively comprise the University's financial statements, and have issued our report thereon dated November 15, 2007. Our report was modified to include a reference to our reliance on other auditors. We conducted our audit in accordance with U.S. generally accepted auditing standards and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Other auditors audited the financial statements of the aggregate discretely presented component units, the University of Arizona Foundation, Inc., the University of Arizona Alumni Association, the Law College Association of the University of Arizona, and the Campus Research Corporation, as described in our report on the University's financial statements. The financial statements of the aggregate discretely presented component units were not audited by the other auditors in accordance with *Government Auditing Standards*. This report includes our consideration of the results of the other auditors' testing of internal control over financial reporting that are reported separately by those other auditors. However, this report, insofar as it relates to the results of the other auditors, is based solely on the reports of the other auditors.

Internal Control over Financial Reporting

In planning and performing our audit, we considered the University's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. However, as discussed below, we and the other auditors identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the University's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the University's financial statements that is more than inconsequential will not be prevented or detected by the University's internal control. We consider items 07-01 through 07-09 described in the accompanying Schedule of Findings and Recommendations to be significant deficiencies in internal control over financial reporting.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the University's internal control.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in internal control that might be significant deficiencies and, accordingly, would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, we believe that none of the significant deficiencies described above is a material weakness.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Managements' responses to the findings identified in our audit have been included herein. We did not audit managements' responses and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of the members of the Arizona State Legislature, the Arizona Board of Regents, and the University and is not intended to be and should not be used by anyone other than these specified parties. However, this report is a matter of public record, and its distribution is not limited.

Debbie Davenport
Auditor General

November 15, 2007

University of Arizona
Schedule of Findings and Recommendations
Year Ended June 30, 2007

University of Arizona Finding

07-01
University of Arizona
The University should improve access controls over its main computer systems

The University processes and stores sensitive student, financial, and personnel data on its main computer systems, which include its student financial aid system (Matrix), the Student Information System (SIS), the Personnel Services Operating System (PSOS), and the Financial Records System (FRS). Therefore, the University should ensure that the access granted to users of these systems is appropriate and limit physical access to IT equipment and stored data. This would help prevent or detect unauthorized use, damage, loss, or modification of programs and equipment, and misuse of sensitive information. However, the University's controls were not always sufficient for preventing and detecting unauthorized access.

Specifically, the University had not established policies and procedures to periodically review whether access levels granted to users of its systems remained appropriate. Also, the University had not established policies and procedures to ensure that it periodically conducted comprehensive reviews of its standard access templates and roles that are used to assign access levels, such as whether a user can add, modify, or delete specific data. Finally, the University had not established standardized policies and procedures for employees to use when they review and approve user access requests and establish access. As a result, auditors found instances where the University inappropriately granted users access to modify and delete sensitive data in Matrix and SIS, and the University could not provide documentation demonstrating who requested and approved access for those two systems.

The following table summarizes the deficiencies over user access controls by system.

Computer System	No university-wide policies and procedures to periodically conduct a comprehensive review of access	No standardized university-wide policies and procedures for employees who review and approve access requests	Inappropriate access granted to users	Insufficient access authorization documentation
Matrix	X	X	X	X
SIS	X	X	X	X
PSOS	X	X		
FRS	X	X		

In addition, the University had not established control procedures that limit and monitor physical access to its central computing Data Center. As a result, auditors noted that at least nine unauthorized employees, including four former employees, had access to the central computing Data Center.

The University should strengthen its policies and procedures over system access to help prevent or detect unauthorized use, damage, loss, or modification of programs and equipment and misuse of sensitive information. Only authorized users should have logical or physical access to the University's computer systems, and access should be limited to essential employees only. While the University currently has certain controls in place over electronic and physical access, implementing the following procedures will significantly strengthen controls:

- Develop university-wide policies and procedures to periodically review users who have access to critical data and to review the standard access templates and roles to help ensure that users' access is appropriate.

- Conduct a comprehensive review of existing users' access and the standard access templates and roles.

- Standardize university-wide policies and procedures that clearly define the responsibilities of employees who are responsible for reviewing, approving, and establishing access, and provide initial and ongoing training to help ensure that the access control procedures are followed.

- Develop access-request, modification, and deletion forms for Matrix. For system access and access change requests, the forms should provide information needed to determine the nature and extent of the user's access, including user's name, title, and department, and access approval from an authorized department employee.

- Improve procedures for removing or modifying access rights of users when they terminate employment or transfer departments.

- Establish policies and procedures to review and monitor physical access to the central computing Data Center.

Component Unit Findings

The other auditors that audited the Law College Association of the University of Arizona and the Campus Research Corporation reported the following significant deficiencies for those component units:

07-02
Law College Association
Investments

As also discussed in the prior year's management letter, no activity was posted to the general ledger during the year, thus transactions occurring outside of the Association on their behalf were unrecorded in the general ledger until year-end. The delay in posting opens the possibility that transactions could have occurred in the investment statements, such as withdrawals or transfers to other accounts, which could have been fraudulent in nature and been undetected until year end. We recommend that all investment activity be recorded and reconciled in the general ledger on a quarterly basis.

Management response: In the future, the Association will post all of the investment activity to the general ledger as investment statements are received. Additionally, the Association has in place other controls to prevent any fraudulent activity in the investment account. 1.) As with all of the LCA accounts, two of three authorized signatures are required to transact any business, no matter how small. 2.) Investments are determined and managed by Northern Trust under the investment policy approved by the LCA Board. 3.) Investment statements are also reviewed when received by the Vice President for Investment, again on a quarterly basis. 4.) The Investment Committee as a whole meets with the Northern Trust fund managers twice a year to review activity and allocation of the investments.

07-03
Law College Association
Cash receipts

It was noted during discussions with a Development Office employee that one individual opens the mail and, if it appears to look like a cash receipt, then that person will open that specific piece with another individual. This first individual also prepares a log of all cash receipts. The Association should implement dual control procedures whereby two individuals open all mail and prepare, date and initial the log together. The log is compared to the subsequent bank deposit by the Administration Assistant. This control would be further strengthened if the individual comparing the log to the bank deposit did not also prepare and record the deposit.

Management response: Procedures have already been changed so that all mail received in the Development Office is opened by two individuals, who photocopy the cash receipts, and prepare, date and initial a log of receipts. Another individual, separate from those who prepare the log and from the Administrative Assistant who prepares the deposits, will reconcile the log to the bank deposits.

07-04
Law College Association
Cash receipts

It was noted during testing that 4 cash receipts selected from 5 bank deposits were not included in the cash receipts log. We recommend making copies of every receipt that is received and include the receipt in the cash receipt log to allow an individual, separate of those opening the mail, to accurately reconcile this log to the deposit summary on a consistent basis. This is a repeat comment.

Management response: Those who prepare the log have been reminded to make sure that a copy of each cash receipt is attached to the log.

07-05
Law College Association
Cash disbursements

7 out of the 25 invoices selected for testing were not signed or stamped for payment. We strongly recommend an authorized individual sign or stamp the invoice to verify the expense has been approved for payment to avoid the risk of paying expenses that are unrelated to the Association.

Management response: All invoices have been and will continue to be reviewed and approved for payment by an authorized individual before a check is prepared. In the future, such approval will be noted on the invoice itself in each case.

07-06
Law College Association
Cash disbursements

During the audit, we noted that for 3 out of the 25 disbursements selected for testing the account numbers to which the expense is to be recorded is not written directly on the invoice prior to printing the checks for payment. We recommend that the general ledger coding be documented and reviewed during the approval process.

Management response: Account numbers were assigned to each invoice before a check was prepared. The account numbers were written on the invoice or on the supporting materials. In the future, the account numbers will be written directly on the invoice if there is sufficient space to do so. The account codes have been and will continue to be reviewed when the check is prepared.

07-07
Law College Association
Voided checks

It was noted during the audit that there were a number of checks voided during the fiscal year for various reasons. The Association was unable to locate approximately 25% of these voided checks. Maintaining physical copies of these checks establishes an audit trail to verify that the checks were actually voided rather than misappropriated and used for unauthorized purchases. We recommend physically voiding the check when it is determined no longer usable, and keeping that check copy on hand as support for confirmation of the void.

Management response: Several checks were voided during the fiscal year as the individuals preparing checks learned how to print checks from the new system (Financial Edge). Each of those checks was voided in the system; the physical check was also voided and then filed. The offices occupied by those who prepare the LCA checks were relocated to another building in May of 2007 while the original facility is being renovated. Many of the files were boxed and marked for temporary storage during the renovation and were not available to the LCA during the period of the audit. The missing physical checks were boxed with some other materials for storage for the LCA. In the future, we will retain the physical voided checks in the file cabinet until the audit is complete (as we have done in the past).

University of Arizona
Schedule of Findings and Recommendations
Year Ended June 30, 2007

07-08
Campus Research Corporation
Financial Statement Preparation

Under recently issued U.S. auditing standards, a company is expected to perform all necessary accounting functions through and including preparation of their financial statements in accordance with U.S. generally accepted accounting principles. Management has determined that it is more effective from a cost/benefit standpoint to outsource the preparation of the financial statements and related footnotes to their auditor instead of internalizing these capabilities. Since the Organization has not internalized these functions, they are considered significant deficiencies in internal control.

Management response: none reported

07-09
Campus Research Corporation
Segregation of Duties

The Chief Operating Officer (COO) is provided with reconciled bank statements by the accounting department for his review monthly. In order to continue to improve the segregation of duties over the Organization's internal controls, we recommend the Organization's bank statements be sent directly to the COO or new Park Director. This will enable him to perform his control function of reviewing the original documents for unusual activity prior to their receipt by the accounting department.

Management response: none reported

Financial Services Office
(520) 621-3220
FAX: (520) 626-6583

THE UNIVERSITY OF
ARIZONA.
TUCSON ARIZONA

University Services Building
888 N. Euclid Ave., Rm. 502
P.O. Box 3310
Tucson, AZ 85722-3310

November 9, 2007

Ms. Debbie Davenport
Auditor General, State of Arizona
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport

The following is the University of Arizona's response to the significant deficiency described in the Schedule of Findings and Recommendations, Item 07-01.

Title of Finding: 07-01 The University should improve access controls over its critical computer systems

Response:

We concur. Please find attached the University's corrective action plan.

I would like to emphasize that we have not responded to items 07-02 through 07-09. These items relate to certain of our component units, which are discreetly presented in the Annual Financial Report of the University. The component units are made up of separate, legal entities that are not subject to management by the University. As such, it would not be appropriate for us to respond to issues pertaining to these entities.

If you have any questions, you may contact me at (520) 626-1677.

Sincerely,

Mark McGurk
Comptroller

Finding: 07-01
"The University should improve access controls over its critical computer systems."
Name(s) of contact person(s): Elizabeth Taylor and Michael Torregrossa
Anticipated completion date(s): (See below)

Planned Corrective Action:

The University will:

- Ensure that the access granted to users of the student financial aid system (Matrix), the Student Information System (SIS), the Personnel Services Operating System (PSOS), and the Financial Records System (FRS) is appropriate
- Limit physical access to critical IT equipment and stored data for student financial aid system (Matrix), the Student Information System (SIS), the Personnel Services Operating System (PSOS), and the Financial Records System (FRS)

By:

1. Developing University-wide policies and procedures to periodically review users who have access to critical data and to review the standard access templates and roles to help ensure that users' access is appropriate.
2. Conducting a comprehensive review of existing users' access and the standard access templates and roles.
3. Standardizing University-wide policies and procedures that clearly define the responsibilities of staff who are responsible for reviewing, approving, and establishing access and provide initial and ongoing training to help ensure that the access control procedures are followed.
4. Developing access request, modification, and deletion forms for Matrix. The forms will require requestors to provide information needed to determine access including name, title, department, supervisor's name, and authorized approver.
5. Improving procedures for removing or modifying access rights of users when they terminate employment or transfer departments.
6. Establishing policies and procedures to review and monitor physical access to the central computing Data Center.

Through:

- The establishment of 2 task forces, charged and scoped by the CIO as follows:

1. **Enterprise Business Systems Physical Access Task Force**

   Charge

   - Review current and best practices and implement a new process in a way that will accomplish item 6 above under centralized oversight

   Scope

   - Consider only central computing Data Center(s) specifically focused on the 4 primary business enterprise systems – Matrix, SIS, FRS and PSOS at this time

   Deliverables

   - Written Policies
   - Written Procedures
   - Identified authority, resources, responsibility and accountability
   - Implementation of full process

   Timeline

   - Task Force will be created, with Chair named by November 1, 2007
   - Recommendations for policies, best practices and resourcing to the CIO by March 1, 2008
   - Policies will be finalized by March 30, 2008
   - Implementation will be complete by end of the June 30, 2008

2. **Enterprise Business Systems Logical Access Task Force**

   Charge

   - Review best practices and implement in a way that will accomplish items 1-5 above under centralized oversight

   Scope

   - Student financial aid system (Matrix)
   - Student Information System (SIS)
   - Personnel Services Operating System (PSOS)
   - Financial Records System (FRS)

   Deliverables

   - Written Policies
   - Written Procedures
   - Identified authority, resources, responsibility and accountability
   - Implementation of full process

   Timeline

   - Task Force will be created, with Chair named by November 1, 2007
   - Recommendations for policies, best practices and resourcing to the CIO by March 1, 2008
   - Policies will be finalized by March 30, 2008
   - Implementation will be complete by end of the June 30, 2008