A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Northern Arizona University

Year Ended June 30, 2009

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

Northern Arizona University
Report on Internal Control and Compliance
Year Ended June 30, 2009

Table of Contents

Page

Report Issued Separately

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

STATE OF ARIZONA
OFFICE OF THE
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 Northern Arizona University as of and for the year ended June 30, 2009, and have issued our report thereon dated October 30, 2009. 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 Northern Arizona University Foundation, Inc., and the Northern Arizona Capital Facilities Finance 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 on 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 identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

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 09-01 through 09-03 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. We believe that none of the significant deficiencies described above is a material weakness. However, certain information came to our attention that we consider to be a material weakness in internal control over financial reporting that has not been included in this report because of its sensitive nature. This information has been provided to the University.

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*.

The University's responses to the findings identified in our audit have been included herein. We did not audit the University's 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 university management 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

October 30, 2009

Northern Arizona University
Schedule of Findings and Recommendations
Year Ended June 30, 2009

Northern Arizona University Findings

09-01
The University should strengthen computer access controls

Criteria: The University should have effective computer access controls to prevent and detect unauthorized use, damage, loss, or modification of programs and data, and misuse of sensitive or confidential information. System access controls restrict not only physical access, but also logical access.

Condition and context: The University uses two main computerized systems to initiate, record, process, and report financial, human resources, payroll, and student information. While performing test work over logical access controls to these systems, auditors noted the following deficiencies:

- The University did not have controls in place to ensure only authorized users had access to sensitive student, financial, and personnel data on its human resources, payroll, and student information system. Specifically, while performing test work on this system, auditors noted that a system password, which allowed access to sensitive data, was stored in an insecure manner.

- The University's database administration team, which consists of five people, uses a shared system administrative user name and password with unlimited privileges, which allowed them the ability to access and change data in the database. The database is the data warehouse for the University's main systems. In addition, the University did not review system activity logs for unauthorized activity.

- The University used a Central Authentication System (CAS) for authenticating system users. The system was supposed to lock out a user after six invalid logon attempts; however, auditors were able to enter incorrect passwords more than six times and were not locked out of the system. In addition, the University has no policies and procedures in place to lock out invalid logon attempts on systems that do not use the CAS for authentication.

Effect: There is an increased risk of theft, manipulation, or misuse of sensitive or confidential data by unauthorized users or by users who were not being properly monitored. This finding is a significant deficiency in internal controls over financial reporting.

Cause: The University's password policies did not restrict the use of stored passwords. Also, the system administrative user name and password was shared as it is more convenient for all database administrators to have access to make changes to the database. In addition, system activity logs were not reviewed because of staffing levels. Further, the University had not enforced their lock-out policy for systems utilizing CAS because of system conflicts and had not developed a policy for account lock-out thresholds for systems that did not utilize CAS.

Recommendation: The University should establish and implement the following policies and procedures to help strengthen system access controls:

- Limit the use of stored passwords and ensure strong encryption methods are used for any passwords being stored.
- Prohibit database usernames and passwords from being shared among system users.
- Maintain and review system activity logs and investigate unusual activity.
- Ensure the account lock-out policy is implemented and utilized on all systems.

09-02
The University should strengthen computer change controls

Criteria: Changes to the University's computer systems should be logged, authorized, tested, and reviewed prior to implementation. Effective change management controls should ensure that program changes and changes to data are valid, meet user needs, and are subject to review and independent approval.

Condition and Context: The University did not have adequate control procedures in place to ensure that all system changes were properly logged, authorized, tested, and reviewed prior to implementation for its main computerized systems that initiate, record, process, and report financial, human resources, payroll, and student information.

Effect: Inadequate program change management could lead to unauthorized changes and changes not applied correctly. Also, gaps between user expectations and business requirements could occur and go undetected. This finding is a significant deficiency in internal control over financial reporting.

Cause: The University did not have adequate control procedures in place to track program changes and ensure that all requests had been authorized, tested, reviewed, and approved.

Recommendation: The University should establish, implement, and enforce formal written policies and procedures to ensure that management and users:

- Log, authorize, test, review, and approve all program changes to computerized systems prior to implementation. In the event of an emergency, ensure the nature of the emergency and that the change made is subsequently documented, reviewed, and approved.
- Monitor all system change requests with a log or report-tracking system to ensure that all requests have been authorized, assigned resources, tested, reviewed, and approved.
- Retain documentation to support that program changes were authorized, tested, reviewed, and approved.

A similar finding was noted in the prior year.

09-03
The University should test its disaster recovery plan

Criteria: It is crucial that the University have an up-to-date and tested disaster recovery plan that would provide continued operations in the case of a system or equipment failure or other interruption. Disaster recovery plans should be tested periodically and modifications should be made to correct any problems to ensure its effectiveness.

Condition and Context: The University's disaster recovery plan, which covers all university computer information systems, had never been tested.

Effect: The University could experience delays in resuming normal operations as the disaster recovery plan may contain flaws that the University is not aware of because the plan has not been tested. This finding is a significant internal control deficiency over financial reporting.

Cause: The University did not test its disaster recovery plan because of a lack of resources.

Recommendation: The University should test its disaster recovery plan periodically and take immediate action to remedy deficiencies that testing identifies.

NORTHERN ARIZONA UNIVERSITY

COMPTROLLER'S OFFICE

December 9, 2009

Debra K. Davenport, CPA
Auditor General
2910 N. 44th Street, Suite 410
Phoenix, AZ 85018

Re: Schedule of findings and recommendations for the Year Ended June 30, 2009.

Dear Ms. Davenport,

Please find attached Northern Arizona University's response to your findings and related recommendations as described in the fiscal year ended June 30, 2009 Schedule of Findings and Recommendations.

Sincerely,

Robert Norton
Associate Vice President

PO Box 4069, Flagstaff, AZ 86011-4069
(928) 523-6054
(928) 523-2052 Fax

Northern Arizona University
Corrective Action Plan
Year Ended June 30, 2009

09-01
The University should strengthen computer access controls
Name(s) of Contact Person(s): Harper Johnson
Anticipated Completion Date/Completion Date: May 2010

Corrective Action Plan:

- Recommendation 09-01a - Limit the use of stored passwords and ensure strong encryption methods are used for any passwords being stored.

  Response 09-01a – A review of stored password usage has been started to ensure that any remaining stored passwords follow the standards requested. The review will be completed by February 2010.

- Recommendation 09-01b - Prohibit database usernames and passwords from being shared among system users.

  Response 09-01b – The database administration team will implement controls to allow for auditing of changes made by individual administrators. This process will be completed by May 2010.

- Recommendation 09-01c - Maintain and review system activity logs and investigate unusual activity.

  Response to 09-01c – The Information Security team in coordination with the ITS system administrators will purchase and implement log monitoring software that will better alert administrators to log anomalies requiring investigation. Completion Date is March 2010.

- Recommendation 09-01d - Ensure the account lock-out policy is implemented and utilized on all systems.

  Response 09-01d – The University's account lock-out rules will be enforced by changes to the Central Authentication System (CAS) by March 2010. A password management policy will be created and implemented for non-CAS systems by May 2010.

09-02
The University should strengthen computer change controls
Name(s) of Contact Person(s): Patrick Benson and Harper Johnson
Anticipated Completion Date/Completion Date: See dates provided in response sections

Corrective Action Plan: *Describe the corrective action planned.*
Comments (Patrick Benson, Director, Administrative Computing):

Agree – This is a complex finding and several efforts are underway to address the recommendations.

- Recommendation 09-02a - Log, authorize, test, review, and approve all program changes to computerized systems prior to implementation. In the event of an emergency, ensure the nature of the emergency and that the change made is subsequently documented, reviewed, and approved.

  Response 09-02a - The Oracle/PeopleSoft application suites have required SOS tickets since 2007. As noted below in the response to Recommendation 2, shortcomings with the current SOS system noted above may have resulted in loss of full information about some changes. This will be addressed with release of the new SOS in June 2010. Policy, vendor supplied and locally extended technology support a robust production environment change management process for Oracle/PeopleSoft application suites. The

Configuration Management Team, CMT, an ITS unit under Computing and Communication Services and independent of the Administrative Computing development teams, controls change implementation.

Subsequent to the AG on-site, management of the CGI/Advantage application suites changed. Effective June 15, 2009 policy requires change requests to be backed by SOS request before they are implemented. A different but equally robust production change management process is in place for Advantage. This process is also under the control of the Configuration Management Team (CMT). Logs and generated reports needed to back up update requests, files are maintained. As with Oracle/PeopleSoft applications, shortcomings with the SOS system are being addressed. As noted below in the response to Recommendation 2, shortcomings with the current SOS system noted above may have resulted in loss of full information about some changes. This will be addressed with release of the new SOS in June 2010.

The Informatica+SAP/BusinessObjects data warehousing reporting application suites will have a CMT-controlled production change management process for institutional reporting in place by December 30, 2010. This process will require SOS tickets be generated to support changes, and SOS tickets will be required to promote changes into the institutional reporting production environment. It is likely that this process will closely resemble the Advantage process described above.

- Recommendation 09-02b - Monitor all system change requests with a log or report-tracking system to ensure that all requests have been authorized, assigned resources, tested, reviewed, and approved.

  Response 09-02b - There is an in-place system to monitor and track change requests, the ITS Service Order System, SOS. The in-place system has shortcomings. Currently, SOS allows an accidental or intentional overlay of information and history. This could result in incomplete or misleading information about a change being retained. This shortcoming is being addressed as a work item in the in-progress rewrite of that system. Specifically, no user will be able to change or delete technical and functional comments after entry. The issue of SOS changes resulting in information overlay identified is being addressed by technology that retains information (including comments, status, etc) uniquely so subsequent or multiple work items do not obfuscate or destroy other or earlier information.

  CITO Fred Estrella has set a June 1, 2010 for the replacement system to be in-place and fully functional.

- Recommendation 09-02c - Retain documentation to support that program changes were authorized, tested, reviewed, and approved.

  See the response to Recommendation 09-02b.

09-03
The University should test its disaster recovery plan
Name(s) of Contact Person(s): Harper P. Johnson
Anticipated Completion Date/Completion Date: March 2010

Corrective Action Plan: The NAU Information Security group will develop and conduct a table top exercise of the ITS Disaster Recovery Plan. The exercise will involve all members of the ITS management team at the Director and Team Lead levels. The goal of the exercise will be to drive awareness of the plan, review its effectiveness, and to make updates to the plan where needed.