A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Arizona State University

Year Ended June 30, 2008

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

Arizona State University
Report on Internal Control and Compliance
Year Ended June 30, 2008

Table of Contents

Page

Report Issued Separately

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 Arizona State University as of and for the year ended June 30, 2008, which collectively comprise the University's financial statements, and have issued our report thereon dated January 9, 2009. Our report was modified to include a reference to our reliance on other auditors and as to consistency because of the implementation of Governmental Accounting Standards Board Statement Nos. 45, 48, and 50. 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 consisting of the Arizona State University Foundation, the Arizona Capital Facilities Finance Corporation, the Arizona State University Alumni Association, the Arizona State University Research Park, Inc., the Collegiate Golf Foundation, the Downtown Phoenix Student Housing, LLC, the Mesa Student Housing, LLC, the Sun Angel Endowment, and the Sun Angel Foundation, 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 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 08-01 through 08-06 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, of the significant deficiencies described above, we consider items 08-01 through 08-04 to be material weaknesses.

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, the University, and 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

January 9, 2009

Arizona State University Findings

08-01
The University needs better controls over payroll expenses and its new human resources and payroll computer system

In July 2007, the University replaced its human resources and payroll system with a new system. This new system was responsible for processing over $861 million in payroll costs during the year, which represented approximately 60 percent of the University's total fiscal year 2008 expenses. Accordingly, when a new system is being implemented, it is imperative for the University to take the necessary steps during the planning phase to design comprehensive internal control policies and procedures and fully train employees on the use of the new system. However, the University did not fully accomplish these objectives, and as a result, the University did not always pay its employees the correct amounts. Specifically, some employees received no paychecks and some received incorrect paychecks resulting in at least $2.4 million in overpayments during the fiscal year. These problems may have been minimized if the University had established comprehensive policies and procedures for monitoring and verifying payroll, performed more thorough testing of the system before implementation, and ensured that employees were adequately trained. Below are some examples of the more significant problems that the University encountered because of these deficiencies.

- For a period of time after implementation, the system was unable to generate reports that departments needed to monitor and verify the accuracy of payroll expenses.

- The system's electronic time clock feature to track and account for employee hours worked did not operate as planned. As a result, many employees were not being paid or were paid incorrect amounts. The University replaced the time clock feature with timesheets that required departmental approval; however, departments did not always approve employees' timesheets in time for paychecks to be processed. Consequently, the University approved timesheets centrally but could not verify actual hours worked. In addition, employees could change hours on their timesheets after they were approved. In June 2008, the University reinstated departmental approval of timesheets, which included approval of changes made to timesheets.

- The University did not have adequate safeguards in place to ensure that additional pay was paid accurately. Additional pay primarily resulted when duties were performed beyond employees' regular assignments or contract terms. However, the duration of time for the additional pay was not always entered into the system by the departments. Further, additional pay was not monitored centrally. Therefore, additional pay was paid to some employees beyond the authorized period, resulting in overpayments. The lack of safeguards also allowed departments to misuse the additional pay feature of the system for making payroll corrections and salary and other adjustments to employees' pay.

- The University did not ensure the system's contract pay component was designed to calculate contract employees' pay accurately when they earned additional pay. Although the majority of contract employees did not earn additional pay, the University ultimately discontinued use of the contract pay component by fiscal year-end due to these complications.

- During system implementation, the University converted all employees from a semi-monthly to a bi-weekly pay cycle. However, in some instances, semi-monthly rates were incorrectly entered into the system instead of bi-weekly rates, resulting in overpayments. In addition, for a period of time, some departments increased employees' pay because they were not aware that the pay cycle had changed and that bi-weekly pay amounts would be less than semi-monthly pay amounts given the same annual salary.

- The University did not always monitor and review salary increases and other changes to ensure they were proper and complied with university-established policies. The Office of Human Resources performed this function until December 2007 when it was delegated to departments; however, the University did not provide written policies and procedures for the departments to follow.

- Certain system-automated checks were not set up to prevent seemingly unreasonable payroll transactions from being entered and processed without review and approval. As a result, an unreasonably large payroll transaction was processed by the system and not detected by the applicable department or the Office of Human Resources during payroll processing. However, this transaction was detected by a manual review performed by the finance department just before the payment was to be made. Better automated checks would help ensure that these types of errors never reach this stage.

- Terminated employees were not always removed from the system in a timely manner and continued to be paid. The University relied on the departments to report when an employee was terminated; however, auditors noted that some overpayments were caused by delays in departments reporting terminations.

- Employee personnel records were not centrally maintained in accordance with university-established policy.

While the University developed policies and procedures for identifying, reporting, and recovering overpayments to employees, it did not implement them until the end of the fiscal year. Further, these policies and procedures did not include detailed instructions for departments to follow to ensure payroll expenses were accurate and all overpayments were identified. Even though the University has successfully recovered most of the identified overpayments, it has referred several overpayments to former employees to collection agencies. In addition, while several departments reported to the Office of Human Resources that some overpayments to employees may have been forgiven, the Office of Human Resources did not follow up timely to ensure that amounts potentially forgiven were collected. If there were any forgiven overpayments, this may constitute a gift of public monies in violation of Arizona Constitution, Article 9, Section 7. Furthermore, the University was unable to identify or track the forgiveness of overpayments because all departments may not have notified the Office of Human Resources of such overpayments.

When implementing the new computer system, the University should have taken the steps and time necessary for ensuring the system and its components functioned as intended and a comprehensive set of internal control policies and procedures was in place. In addition, the University should have ensured that its employees were fully trained on the system's use and understood the steps necessary to process payroll, such as entering hours worked, reviewing and approving time recorded, and making salary adjustments. Furthermore, the University needed better procedures to support that existing data from the old system was properly entered into the new system. Finally, the University should have ensured that the system was able to generate the reports needed by departments for monitoring and verifying payroll expenses. To help ensure payroll transactions are accurately recorded, processed, paid, and reported in its financial statements, the University should:

- Establish a comprehensive set of policies and procedures for monitoring and verifying payroll expenses. These policies should include detailed procedures for identifying, reporting, and recovering overpayments to employees.
- Continue efforts to investigate and recover overpayments, including those forgiven by departments and those referred to collection agencies.
- Ensure that departments are aware of and follow guidelines for verifying and approving time recorded by employees in accordance with established schedules for processing payroll.
- Improve controls over processing contract pay, additional pay, payroll corrections, and other adjustments to employees' pay to ensure their propriety.
- Provide written policies and procedures to departments for performing independent reviews of salary and other changes to ensure that they are proper and comply with university-established policies.
- Install system-automated checks to prevent unreasonable payroll transactions from being entered and processed without review and approval.
- Remove terminated employees from the system in a timely manner to ensure that they are not paid inappropriately.
- Adhere to university-established policies by centrally maintaining employee personnel records.

08-02
The University should strengthen controls over security, access, and change management for its new computer systems

The University implemented two systems, a student information system in April 2007 and, as discussed in item 08-01, a human resources and payroll system in July 2007. The systems initiate, record, process, and report financial data related to human resources, payroll, and student enrollment and financial assistance. These systems also contain sensitive and confidential information, such as employees' and students' social security numbers. Therefore, it is critical that these systems and the information they contain are secured and protected from unauthorized access, use, and modification. However, the University did not have adequate internal controls over system security, logical access, and change management.

Security
Information technology security practices are important to protect the University's computer systems and the sensitive and confidential information which is stored on them, including information associated with over 64,300 students and nearly 25,000 faculty and staff. The University entered into an agreement with an

out-of-state service organization to host its systems, thereby utilizing the service organization's facilities and hardware to run its applications. Services provided by this organization were done with the assumption that certain internal controls would be implemented by the University. However, the University did not fully implement all of the controls that were necessary to complement the service organization's controls. In particular, the University did not have a formal business continuity strategy and written policies and procedures for assessing, identifying, and mitigating security risk for its systems and had not performed a security risk assessment of these systems.

Logical Access
Logical access controls, such as those associated with identification, authentication, and authorization, are critical for protecting sensitive information and preventing and detecting unauthorized use of and modification to systems and the data they contain. Proper logical access controls help ensure that only authorized users have the ability to read, create, or modify data in a system, and that no one individual has the ability to make changes to critical data without an independent review. The University required users to have unique identifications and passwords to gain access to its human resources and payroll and student information systems. However, the University did not install the automated lock-out features on these systems, leaving them vulnerable to unauthorized access through deliberate and persistent attempts to gain access. Further, the University did not have adequate procedures for removing users' system access after users terminated employment or transferred jobs within the University. Finally, the University did not have procedures for defining, assigning, and approving user access roles and responsibilities in the system to ensure proper separation of responsibilities. For example, auditors noted two employees who were involved in the system's development and implementation who also were able to make changes in the human resources and payroll system, such as adding employees or increasing salaries, and process payroll.

Change Management
To help ensure that an information system functions as designed, it is essential that program changes to the system be properly documented, authorized, tested, and approved before modifications are made. Although program changes are necessary to ensure systems continue to function as intended, particularly when implementing new systems, the University did not have adequate written policies and procedures for making and implementing changes to its human resources and payroll and student information systems. While program changes are made by the University's out-of-state service organization, it is the responsibility of the University to manage and test any system modifications prior to being put into use. Auditors noted several instances for which the University did not have documentation or other evidence to support that it approved the changes. In addition, the University did not test program changes and, as a result, it did not document testing procedures and test results. Further, the University did not require system changes, including those initiated by the service organization, to be independently reviewed to verify that changes were consistently documented, authorized, tested, and approved before being put into use.

To help strengthen controls over security, access, and change management for its new computer systems, the University should:

Security

- Establish a formal business continuity strategy.
- Develop and implement written policies and procedures for assessing, indentifying, and mitigating security risks for the systems.
- Perform a security risk assessment of the systems, including the Web-based applications used to grant access to these systems, as mentioned in item 08-03.

Logical Access

- Implement automated features within the systems to lock-out users' access accounts after a certain number of failed access attempts in order to reduce the likelihood of unauthorized access by potential attackers.
- Remove users' system access immediately after users terminate employment or are transferred to other jobs within the University.
- Develop procedures to ensure proper separation of responsibilities by defining, assigning, and approving user access roles and responsibilities in the systems.

Change Management

- Develop and implement written policies and procedures for making program changes to the systems. These procedures should require that program changes are documented, authorized, tested, and approved prior to implementation.
- Perform an independent review of all system changes, including those initiated by the service organization, to ensure that those changes are consistently documented, authorized, tested, and approved before being put into use.

08-03
The University needs to improve controls over its Web-based application used to grant access to its computer systems

The human resources and payroll and student information systems contain financial information that is reported in the University's financial statements. They also contain personal sensitive information, such as student, faculty, and staff social security numbers. One particular Web-based application is used to provide system users with access to these systems. As reported in the Auditor General's performance audit report, *Arizona's Universities—Information Technology Security*, this Web-based application was vulnerable because a combination of weaknesses could allow unauthorized access to the University's computer systems and the sensitive financial and personal information they contain. In addition, the University had not performed a security risk assessment of the Web-based portions of the payroll and student information systems as mentioned in item 08-02.

While the University has taken corrective action to address the specific Web-based vulnerabilities identified in our performance audit report, these security weaknesses existed for most of the fiscal year. The University should continue its efforts for ensuring its systems and financial and sensitive information they contain are protected from unauthorized access and use. Additionally, these efforts should specifically include performing security assessments of the Web-based portions of the human resources and payroll and student information systems. The University should also develop procedures to ensure security reviews are conducted on a regular basis, to assess whether security controls are functioning effectively, and to ensure problems found are resolved.

08-04
The University should strengthen controls over access, program changes, and disaster recovery for its financial accounting system

The University's financial accounting system is central to its daily operations. Faculty and staff use the financial accounting system to order goods and services, bill departments for goods and services provided, fiscally manage sponsored program research accounts, summarize transactions recorded on the University's other systems, and prepare its financial statements for the public and stakeholders. However, the University did not have adequate internal controls over logical access, program changes, and disaster recovery to protect this system against data loss; to prevent unauthorized access to, use of, and changes to the system; and to ensure that operations continue and information is recovered in the event of a disaster.

Logical Access
Logical access controls are critical for preventing or detecting unauthorized use of and modification to systems and the data they contain. Proper logical access controls help ensure that only authorized users have the ability to read, create, or modify data in a system, and that no one individual has the ability to make changes to critical data without an independent review. Thus, the activities of users, particularly those individuals having high levels of system access, should be monitored. However, the University did not monitor the activities of two employees having high levels of system access, including the ability to change data directly within the database. Further, database changes were not documented, monitored, or properly authorized. In addition, the University did not deactivate an employee's administrative access privileges after placing the employee on administrative leave and relieving the employee of his or her duties; however, the University removed this individual's access upon notification by the auditors. Finally, the University did not maintain a complete and accurate listing or history of users with access to the financial accounting system. Auditors noted that there were employees with access that were not on the University's authorized user list.

Program Changes
Effective change management controls should ensure that program changes and changes to financial data are valid, meet user needs, and are subject to review and independent approval. Additionally, it is important to maintain a separation of responsibilities between the individual programmers who develop and test the program changes and the employees who implement the changes. However, this was not done. Also, computer program change requests were not initiated in writing or otherwise documented. In addition, testing procedures, test results, and final approvals to put changes into use were not always documented. Finally, there were no independent reviews of program changes.

Disaster Recovery
Effective disaster recovery ensures that critical systems can continue if hardware or software fails or other interruptions occur. It is critical for the University to have an up-to-date disaster recovery plan in place to provide continued operations and business continuity in the event of a major system failure or disaster. However, the University's disaster recovery plan for its financial accounting system has not been updated and tested since April 2006.

To help protect its financial accounting system against data loss, help prevent unauthorized access and changes to the system, and to help ensure operations continue and information is recovered in the event of a disaster, the University should:

Logical Access
- Monitor the activities of those employees having high levels of system access, including the ability to change data directly within the database. Further, changes to critical fields in the database should be documented and monitored to ensure all changes are properly authorized. Access to this documentation should be restricted so that employees with the ability to make database changes cannot change the documentation.
- Revoke all access privileges for employees who are placed on administrative leave immediately.
- Ensure that existing procedures for controlling and granting access to the financial accounting system provide the University with the ability to accurately identify all users having system access at a given point in time.

Program Changes
- Document, authorize, test, review, and approve program changes to the system before they are put into use.
- Ensure that an adequate separation of responsibilities exists between those who authorize, design, and develop program changes and those who put the changes into use.

Disaster Recovery
- Review update, and test the disaster recovery plan for the financial accounting system at least annually.

Component Unit Findings

The other auditors who audited Arizona State University Foundation and the Sun Angel Foundation reported the following significant deficiencies for those component units.

08-05
Arizona State University Foundation
Audit Adjustment

In conformity with APB Opinion No. 21, *Interest on Receivables and Payables*, the discount rate that is determined at the time the pledges receivable are initially recognized should not be revised subsequently. During 2008, the discount rates used to calculate the present value for fiscal year 2008 on pledges receivables recognized in prior years were not consistent with the discount rates previously used to calculate the present value on those same pledges receivable in prior years. Accordingly, an audit adjustment was proposed to correct this error. The effect of this adjustment was to increase the discount on pledges receivable and decrease contribution support by approximately $4,100,000. We recommend that management implement a control procedure that would provide for the review of the calculation of the present value discount on long-term pledges receivable by a member of the accounting staff who is at an appropriate level to detect such errors.

Management response: Foundation management agrees with the findings described above. The discount rates used to calculate the present value of the pledges receivable were inadvertently taken from an earlier version of the discount calculation, which had been used to analyze an alternative method for quantifying pledges receivable. The incorrect rates were not identified during review of the final calculation. The accounting staff has been educated and an additional review process has been implemented to ensure that correct rates are used in the future. Additionally, this calculation will be performed and reviewed periodically throughout the fiscal year in order to identify problems and to allow staff to calculate this more frequently, enabling better understanding and review.

08-06
Sun Angel Foundation
Prior Period Pledge Receivable Revision Not Recorded

During 2008, the Foundation recognized a contribution that was received in a prior period. Periodically, donors may decide to make revisions to their unpaid promises to give. In 2007, one donor made such a revision by increasing their unconditional promise to give by $100,000. Certain members of management were aware of the pledge revision; however, the information was not captured in the 2007 financial statements. As a result, the contribution was improperly recognized in the June 30, 2008 financial statements. Management considered the effects of the improper recognition of this pledge revision on the 2008 and 2007 financial statements, taken as a whole, to be more than inconsequential, but less than material, and accordingly no adjustments were made to the 2007 or 2008 financial statements. The Foundation should implement controls that require communication between program and accounting personnel regarding all changes and additions of promises to give. Also, the Foundation should reconcile the schedule of pledges receivable to the general ledger on a monthly basis and have it reviewed by program and accounting personnel to ensure its completeness and accuracy.

Management response: The Foundation currently has a system in place to better track its pledges receivable and any subsequent changes to those pledges than it did at the end of fiscal year 2007 when this error occurred. The error described above represents 0.5 percent and 0.6 percent of total revenues and support for the years ended June 30, 2008 and 2007, respectively. Although the Foundation feels that this amount is not material, it recognizes the importance of ensuring that its pledges are recorded and monitored appropriately.

ARIZONA STATE UNIVERSITY
FINANCIAL SERVICES
PO BOX 877505
TEMPE, AZ 85287-7505
(480) 965-7228
FAX: (480) 727-9922

April 7, 2009

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

Dear Ms. Davenport:

Arizona State University's responses to the findings and recommendations, and related corrective action plans and current status, in conjunction with the financial audit for the year ended June 30, 2008 are enclosed.

As can be seen by review of our responses, the vast majority of the situations noted have already been completely rectified.

If there are any questions on our responses, please contact us.

Sincerely,

General E. Snyder
Senior Associate Vice President for Finance and Deputy Treasurer

Enclosure

c: Morgan R. Olsen, Executive Vice President, Treasurer and CFO
Adrian Sannier, University Technology Officer and VP
Matthew McElrath, Associate Vice President, Human Resources

Arizona State University

Responses to the Findings and Recommendations, and Related Corrective Action Plans and Current Status, in Conjunction with the Financial Audit for the Year Ended June 30, 2008
(Responded to in order as presented in the Auditor General's Report)

Finding 08-01: The University needs better controls over payroll expenses and its new human resources and payroll computer system.

In regard to the deficiencies noted by the auditors in finding 08-01, ASU's response and current status are as follows:

- It was noted that for a period of time after implementation, the system was unable to generate reports that departments needed to monitor and verify the accuracy of payroll expenses. This noted deficiency in not having the needed reports was rectified in the second half of fiscal year 2008. An HR expenditure report listing specific payroll expenses in relation to department budget was developed. Additionally, the following tools to assist the departments in monitoring and reviewing their payroll expenses were put into place throughout fiscal year 2009:
    - Policy FIN 203 – Org Manager Responsibilities – describes the accountability for departments to ensure their payroll expenses are accurate in accordance with their respective budgets.
    - Business Process Guide - to assist in reconciling Payroll Expenses
    - Policy SPP 405-02 – Overpayment – addresses the process to follow in the event an overpayment has been determined.
- It was noted that there was initially centralized approval of timesheets for certain employees and not departmental approval. This noted deficiency of not having departmental approvals for all employees was rectified in the second half of fiscal year 2008. The ability for employees to change reporting of hours worked after departmental approval was removed, along with the centralized approvals of all timecards, by the end of June 2008. During the timeframe where centralized approvals were processed, an extremely low percentage, only 1.7%, of total employee hours, was paid prior to departmental approval. This was done to ensure timely payment of wages to employees during the initial system implementation. Currently, approval of an employee's time worked must be completed at the departmental level. If the department does not approve the time within the required payroll processing deadline, the un-approved time will not be brought forward for payment in the payroll system until the department submits a payroll correction to pay the employee for the subsequently approved time worked.

- It was noted that there were not adequate safeguards in place to ensure that employees with earnings in addition to their regular salaries and wages had these additional earnings processed correctly. This noted deficiency was rectified in the third quarter of fiscal year 2009. The university developed an on-line Payroll Correction Form. This form enables departments to submit pay corrections, along with salary and other adjustments to employees' pay, while providing controls to minimize any potential departmental misuse of the additional pay feature. The university is centrally monitoring additional pay through the Payroll Online Correction Form approval routing.

- It was noted that there were problems with the contract pay component of the new system. As noted by the auditors, this deficiency was rectified by discontinuing the contract pay component during the second half of fiscal year 2008. The human resources and payroll system contract pay module did not function as anticipated when the system was configured initially. While the vast majority of faculty were paid correctly, the contract pay module did not perform adequately when a faculty member received any additional pay during the contract period (e.g. for teaching an additional class). Consequently, all faculty were converted to the standard bi-weekly payroll schedule.

- It was noted that there was some incorrect conversions to the new system of semi-monthly pay rates. This noted deficiency was rectified during the first half of fiscal year 2008. At the time of the new human resources and payroll system initial implementation, the university transitioned from a semi-monthly to a bi-weekly pay frequency. Nationally this is the most common pay frequency and also is the pay frequency used by the other two Arizona universities. Coupled with this change, the university also moved to a schedule where pay dates are one week after last time worked. This change resulted in an initial three-week lag to transition between pay dates. The university made the decision to phase in the new pay frequency change over three pay periods, utilizing a method where a portion of the employee's pay was based on actual hours with the remaining pay based on estimated hours. This was done to lessen the financial burden on employees in making this pay frequency change. This phasing in of the change in pay cycles significantly complicated the pay frequency conversion, but only lasted for six weeks. Unfortunately as a result of the pay frequency change, some departments inadvertently increased employees' initial pay. This situation was corrected shortly thereafter.

- It was noted that there was lack of monitoring by the Office of Human Resources of salary increases and other changes to the employee database. This noted deficiency was rectified during the third quarter of fiscal year 2009. Prior to implementation of the new human resources and payroll system, the previous, legacy system allowed for department-based approval and data entry of salary increases and other changes. Upon implementation of the new human resources and payroll system, the university has changed its business processes to provide for the central review and approval of salary adjustments and changes. Under development are more systematic audit triggers to prompt review and approval of adjustments and changes that exceed established thresholds, before the changes are implemented. This further enhancement has an anticipated implementation of first half fiscal year 2010. In addition, departments are continuously being educated on the required documentation and authorization for all human resources and payroll transactions, which must be maintained on file.

- It was noted that automated edit checks were not installed in the initial system implementation to prevent or detect obviously incorrect payroll transactions. This noted deficiency was rectified during the first half of fiscal year 2008, shortly after this oversight was noted by the auditors. The payroll management team now runs a regular query of the checks currently in process to review gross amounts to be received. This list is then reviewed by the appropriate payroll representative and signed off by the payroll supervisor. Adjustments for any errors identified are made prior to payroll confirmation. Payroll edits are in place via university reporting tools to identify any high dollar amounts. In December 2008, the query was further broken out into each pay group to set different dollar limits (e.g., students have a lower threshold than faculty). The query automatically sends an email to appropriate Office of Human Resources payroll staff.

- It was noted that terminated employees were not always removed from the system in a timely manner. This noted deficiency was rectified during the first half of fiscal year 2009. With the implementation of the new human resources and payroll system, the ability to control when an employee terminates is processed at the department level. Departments have the ability to audit and verify their payroll expenses for employees who will be paid with each upcoming payroll, the Wednesday before the actual pay date. They can utilize reports available through university report tools. In addition, the Office of Human Resources has implemented an auto termination process, which automatically terminates an employee record if there has not been activity for more than four months. This four-month timeframe allows for employees not being paid over the summer to remain an active employee as long as they return in August, with automatic termination if they do not return.

- It was noted that employee personnel records were not centrally maintained in accordance with university-established policy. This noted deficiency is scheduled to be rectified during the first half of fiscal year 2010. ASU will be requesting that departments provide the documentation of employee personnel files to the Office of Human Resources, and also will communicate the importance of centrally housing the personnel files, in compliance with current policy SPP 1101 – Personnel Records. Even though this action has a target completion date of the first half of fiscal year 2010, the long-term objective is to be able to electronically store employee personnel data, which will better address the noted deficiency and sufficiently reduce the decentralization of personnel records.

The auditors made several recommendations in conjunction with finding 08-01. ASU's response and current status of each finding are as follows:

- Establish a comprehensive set of policies and procedures for monitoring and verifying payroll expenses. The following four tools to assist departments in monitoring and reviewing their payroll expenses have been put into place throughout fiscal 2009:

- Policy FIN 203 – Org Manager Responsibilities: Describes the accountability for departments to ensure their payroll expenses are accurate in accordance with their respective budgets.

- MyReports – HR Expenditures: Reporting of departmental payroll expenses in relation to their budget.

- Business Process Guide: Assists in reconciling Payroll Expenses.

- Policy SPP 405-02 – Overpayment: Addresses the process to follow in the event an overpayment has been determined.

- <u>Investigate and recover payroll overpayments.</u> This recommendation is substantially completed. Out of the total $2.4 million in overpayments identified, the vast majority has been collected (all but $65,000 or 2.7% of the total overpayments). The identified $2.4 million in overpayments represents only .003% (3/10 of 1%) of ASU's total annual payroll. The Office of Human Resources is currently and continuously working on the remaining recovery of overpayments from current and former employees Even though some departments wanted to forgive certain overpayments, all overpayments known by Human Resources have now either been collected or are in active collection status. The process for recovery of overpayments is as follows:

  - Current Employees – Overpayments, once identified, are recovered through payroll deductions, or the employee may submit a personal check for the repayment of the overpayment if the check is expediently received.

  - Former Employees - The Payroll Department sends a sequence of three request for repayment letters. If there is no response from the former employee, the case is then referred to ASU's internal collections department. The internal collection department then attempts to make contact with the former employee once again. If there is no response within 30 days, the case is then referred to an outside collection agency and reported to credit bureaus.

  The responsibility for departments to identify all overpayments and the process for collecting on overpayments were clarified to departments through the issuance of a policy on this subject in July 2008.

- <u>Ensure that departments verify and approve all time recorded by employees.</u> This recommendation was implemented during the second half of fiscal year 2008. In June 2008, the University reinstituted departmental approvals of timesheets University-wide, including a review of any changes made to timesheets after the initial approval. Due to the department-based data entry for hours worked, this approval requires continuous monitoring and is constantly being addressed to ensure that all time records get approved in the timeframe determined by the payroll department in order to pay the employee in a timely manner.

- Improve controls over processing contract pay, additional pay, payroll corrections, and salary and other adjustments to employees' pay to ensure their propriety. ASU implemented an online pay correction form during the third quarter of fiscal year 2009. This form enables departments to submit pay corrections, additions, adjustments or indications of overpayment situations directly on the form. This form eliminates the erroneous entry of earnings codes and controls the entry a department has the ability to complete. This form is then routed through the appropriate approvals in order to be processed within the payroll system.

- Provide written policies and procedures to departments for performing independent reviews of salary and other changes to ensure that they are proper and comply with university-established policies. This noted deficiency was rectified during the third quarter of fiscal year 2009. Prior to implementation of the new human resources and payroll system, the previous, legacy system allowed for department-based approval and data entry of salary increases and other changes. Since implementation of the new human resources and payroll system, the university has improved business processes for the review and approval of salary adjustments and changes. The university currently has policies in place that address rates of pay (SPP 403-02) and also salary adjustments (SPP 403-08), with the later policy having been recently revised and updated. Another tool which departments can use for determining salary changes is the Compensation and Salary Administration – Guideline for Managers document located on the Compensation page of the Human Resources web site. The compensation section of Human Resources periodically performs a variety of internal audits of salary administration practices to provide analysis to management regarding adherence with established policies.

- Install automated edit checks in the system to prevent large or incorrectly entered payroll transactions from processing without review or approval. This recommendation was implemented during the first half of fiscal year 2008, shortly after this oversight was noted by the auditors.

- Remove terminated employees from the system in a timely manner. As previously mentioned, this recommendation was implemented during the first half of fiscal year 2009.

- Adhere to university policy by centrally maintaining employee records. As previously mentioned, this recommendation is scheduled to be completed during the first quarter of fiscal year 2010.

Finding 08-02: The University should strengthen controls over security, access, and change management for its new computer systems.

In regard to the deficiencies noted by the auditors in Finding 08-02, ASU's responses and current status are as follows:

- Security - The university had not fully implemented all of the required complementary user organization controls. The noted deficiency regarding Complementary Controls was rectified during the third quarter of fiscal year 2009. ASU has completed the Complementary Controls portion of the Cedar/Crestone hosting service agreement, which includes completing its formal business continuity strategy. ASU will complete a security risk assessment during the fourth quarter of fiscal year 2009 and is developing a schedule and plan for future assessments.

- Logical access - The university did not install automated lock-out features on its systems, leaving the systems vulnerable, and did not have adequate procedures for removing access after users terminated employment or transferred to other jobs within ASU. The rectification of noted deficiencies is well underway, with planned completion during the fourth quarter of fiscal year 2009.

  For the past 20 years, ASU's ASURite login system has allowed repeated attempts without a lockout feature. In that time, there is no evidence that this vulnerability was ever successfully exploited. Nevertheless, ASU accepts as a best practice that its login system should mitigate risk of deliberate and persistent attempts to gain unauthorized access to ASU systems through the implementation of Captcha technology. This project, to implement Captcha comprehensively into all ASURite logins, is underway and will be completed in the second half of fiscal year 2009.

  Prior to the second half of fiscal year 2008, the procedure for removing a terminated employee's system access was driven by departmental request. ASU accepts as a best practice that automated termination processing is a preferred solution. This noted deficiency was rectified during the second half of fiscal year 2008.

  With respect to employee transfers, ASU is documenting the process for review of appropriate authorizations to realign system access for transferred employees where appropriate. Through this process, this deficiency will be rectified during the second half of fiscal year 2009.

  At the conclusion of the human resources and payroll system implementation in the second half of fiscal year 2008, ASU instituted full separation of duties between those responsible for system development and implementation, and those with the ability to make changes in the human resources and payroll system, such as adding employees or increasing salaries, and processing payroll.

- Change management - The university did not have adequate written policies and procedures for making program changes. This noted deficiency was rectified during the third quarter of fiscal year 2009.

  Until the first half of fiscal year 2009, ASU's written policies and procedures for implementing changes to its human resources / payroll and student information systems were decentralized. ASU has since completed a project that centralized all documentation for development of its human resources / payroll and student information systems.

During the implementation of ASU's new human resources and payroll and student information systems, ASU performed comprehensive system and functional level testing in accordance with industry best practices. Proof of successful functional testing was required prior to production migration. ASU documented these approvals but accepts that it did not retain documentation of the test results that supported those approvals.

To address this deficiency, ASU has implemented documented electronic test plans associated with each project. The university continues to require that all changes be logged, authorized, tested and approved prior to implementation. To document this long-standing requirement, ASU has improved the business process which tracks these activities.

To better document the independent review of all system changes, ASU has implemented a tracking procedure. All system changes require documentation of technical review. Hosting service changes are applied during scheduled maintenance cycles. Each item goes through a review cycle between ASU and its hosting provider. Once the implementation is complete, ASU documents the results of the Initial Verification Test (IVT) followed by a post-implementation review.

The audit report contains several specific recommendations in conjunction with Finding 08-02.

<u>Security</u>

- <u>Establish a formal business continuity strategy.</u> This recommendation was implemented during the third quarter of fiscal year 2009.

- <u>Develop and implement written policies and procedures in regard to security risks for the systems</u>. This recommendation was implemented during the third quarter of fiscal year 2009.

- <u>Perform a security risk assessment of the systems, including those web-based applications used to grant access to these systems, as mentioned in finding 08-03.</u> This recommendation will be implemented during the fourth quarter of fiscal year 2009.

<u>Logical Access</u>

- <u>Install automated features within the systems that lock-out users' access accounts after a certain number of failed login attempts, to reduce the vulnerability to unauthorized access.</u> This recommendation will be implemented during the fourth quarter of fiscal year 2009.

- <u>Remove users' system access immediately after users terminate employment or are transferred to other jobs within the University.</u> The recommendation relative to terminated employees was implemented in the second half of fiscal year 2008. With respect to employee transfers, ASU is documenting the process for review of appropriate authorizations, to realign system access for transferred employees where appropriate.

Through this process, this recommendation relative to transferred employees will be implemented during the fourth quarter of fiscal year 2009.

- Develop procedures to ensure proper segregation of responsibilities by defining, assigning and approving user access roles and responsibilities in the system. This recommendation was substantially implemented at the conclusion of the human resources and payroll system implementation in the second half of fiscal year 2008.

Change Management

- Develop and implement written policies and procedures for making program changes to the systems. This recommendation was implemented during the third quarter of fiscal year 2009.

- Review and monitor all program changes made by the contracted service organization to ensure that those changes are logged, authorized, tested and approved before implementation. This recommendation was implemented during the third quarter of fiscal year 2009.

Finding 08-03: The University needs to improve controls over its Web-based application used to gain access to its computer systems.

In regard to the deficiencies noted by the auditors in finding 08-03, ASU's responses and current status are as follows:

Until the second half of fiscal year 2008, for a period of more than 10 years, the web-based application that provides ASURite login had a vulnerability based on a combination of weaknesses that could allow unauthorized access. In that time, there is no evidence that this vulnerability was ever successfully exploited. ASU fixed this vulnerability within hours of becoming aware of its existence.

ASU continues its efforts to ensure its systems and sensitive information they contain are protected from unauthorized access and use. Additionally, ASU performs semi-annual security assessments of the web-based portions of the human resources and payroll and student information systems.

Finding 08-04: The University should strengthen controls over access, program changes, and disaster recovery for its financial accounting system.

In regard to the deficiencies noted by the auditors in finding 08-04, ASU's responses and current status are as follows:

- Logical Access - The university did not have adequate access controls for its financial accounting system. This noted deficiency was rectified during the first half of fiscal year 2009.

  ASU has been using the same financial system with the same financial controls for the past twenty years. For most of the life of that system, two individuals have maintained and supported it. During that time, there have been no audit findings relative to controls.

  ASU accepts as a best practice that changes to the database should be logged, monitored and properly authorized. The individuals referenced by the auditor were trusted members of the ASU team that were uniquely qualified to support this system. Even when one of those individuals was placed on administrative leave because of planned retirement, it was with the understanding that he was on-call for production support of the financial accounting system, due to the highly specialized nature of his skill. His access was removed in August, 2008 with the employee retiring shortly thereafter.

  ASU maintains that this individual's access to financial accounting system was appropriate until the time of his retirement. ASU accepts, however, the appearance of impropriety that could arise in this situation. ASU now rescinds access to the financial accounting system for any individuals on administrative leave.

  ASU does maintain a complete and accurate listing of users with access to the financial accounting system. ASU regrets that the information first provided during the research phase of the audit was inaccurate, but contends that it is not a reflection of the accountability or accuracy of the record of users provided access to the financial accounting system. A complete and accurate list of current users with access to the financial accounting system is being provided to the auditors.

- Program changes - The university did not have adequate change management controls, including review and independent approval. This noted deficiency was rectified during the first half fiscal year 2009.

  ASU has been using the same financial system with the same change management controls for the past twenty years. During that time, there have been no audit findings relative to controls. ASU has, however, implemented a full set of improved procedures incorporating checks and balances for applying changes to the financial accounting system, so that there will not be any future problems in this area.

- Disaster recovery - The university's disaster recovery plan for its financial accounting system had not been updated annually. This noted deficiency was rectified during the third quarter of fiscal year 2009.

  ASU has been using the same financial system with the same disaster recovery procedure for the past twenty years. During that time, including several disasters, there has never been an occasion where data was unrecoverable. In the third quarter of fiscal year 2009, ASU exercised its twenty-year old disaster recovery procedures successfully. The financial accounting system was fully restored and testing confirmed its complete success.

The auditors made several recommendations in conjunction with finding 08-04. ASU's response and current status of each finding are as follows:

Logical Access

- Monitor the activities of those individuals having a high level of system access, including the ability to change data directly within the database. This recommendation was implemented during the first half of fiscal year 2009.

- Immediately revoke all access privileges for individuals who are placed on administrative leave and relieved of duties. This recommendation was implemented during the first half of fiscal year 2009.

- Ensure that existing procedures for controlling and granting access to the financial accounting system provide the university the ability to accurately identify all users having system access at a given point of time. This recommendation was implemented during the first half of fiscal year 2009.

Program Changes

- Log, authorize, test, review, and approve modifications to the system prior to implementation. This recommendation was implemented during the first half of fiscal year 2009.

- Ensure that an adequate separation of duties exists between the authorization, design, and development of the program change on one hand, and the approval to move the change into production on the other. This recommendation was implemented during the first half of fiscal year 2009.

Disaster Recovery

Update and test its disaster recovery plan for its financial accounting system annually. This recommendation was implemented during the third quarter of fiscal year 2009.