A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Arizona State University

Year Ended June 30, 2009

INTEGRITY ★ ACCOUNTABILITY ★ MAKING A DIFFERENCE
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

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

Table of Contents

Page

Report Issued Separately

2009 Financial Report

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, 2009, which collectively comprise the University's financial statements, and have issued our report thereon dated November 25, 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 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, the Sun Angel Foundation, and the University Public Schools, Inc., 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.

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. However, of the significant deficiencies described above, we consider items 09-01 and 09-02 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*.

The University's responses to the findings identified in our audit are 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

November 25, 2009

09-01
The University should strengthen controls over payroll expenses

Criteria: The University needs to have strong internal controls in place to accurately process and record payroll expenses.

Condition and context: The University's payroll and related expenses comprise over $873 million, or approximately 60 percent, of its total expenses. When obtaining an understanding of the University's internal control over payroll expenses and testing those controls, auditors noted the following deficiencies:

- A comprehensive set of policies and procedures for processing, monitoring, and verifying payroll expenses had not been established. For example, the University did not have policies and procedures providing departments instructions for processing payroll, such as verifying the accuracy of employee payroll data, reviewing and approving time recorded, calculating faculty summer pay, and retaining supporting documentation for employee payroll changes.

- For 56 of 81 university departments where employees were selected for test work, the department did not follow the University's policies requiring monthly detailed reconciliations of payroll expenses for each employee to the terms of their employment agreements.

- For 6 of 107 employees selected for test work, the employee was not paid or reimbursed for employment-related expenses in accordance with their employment contract, offer letter, or other official documentation maintained in their personnel file.

- Annual contract renewals for faculty and academic professionals were not formally documented using a Notice of Appointment form in accordance with university and Arizona Board of Regents' policies.

- For one unit within the Office of Human Resources and 3 of 81 departments where employees were selected for test work, timesheets for hourly employees were approved by employees who did not have firsthand knowledge of the actual time worked. Further, certain university employees were assigned rights within the payroll system to centrally approve timesheets for any employee; however, these rights should have been limited to appropriate employees within the payroll unit of the Office of Human Resources.

- Leave requests for exempt employees were not always reviewed and monitored at the department level since some departments had not established adequate policies and procedures.

- Salary increases and additional pay, such as bonuses, pay-related reimbursements, and pay for duties performed beyond an employee's regular assignments or contract terms, were not monitored from July 2008 through December 2008 to ensure employees were paid accurately.

- Payroll overpayments were not monitored by the University to ensure that a complete overpayment listing was maintained, overpayments were collected in a timely manner, and recurring reasons for overpayments had been determined and corrected.

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

Effect: The lack of internal controls over payroll expenses may result in misstating the financial statements or paying employees wrong amounts. In addition, it also increases the risk of fraudulent payroll transactions occurring and not being detected. This finding is a material weakness in internal control over financial reporting. However, auditors were able to perform sufficient alternate procedures to determine that payroll expenses were not materially misstated.

Cause: The payroll processing function is highly decentralized at the University, and the University did not have comprehensive policies and procedures for the departments to follow. Further, the University did not effectively monitor the decentralized payroll functions creating additional internal control deficiencies.

Recommendation: To help ensure payroll transactions are accurately processed and recorded, the University should:

- Establish a comprehensive set of policies and procedures for processing, monitoring, and verifying payroll expenses.

- Ensure that all departments prepare monthly reconciliations of payroll expenses for each employee to the terms of their employment agreements.

- Improve controls over employee payroll to ensure that pay data reflected in the payroll system is supported by the contract, offer letter, or other official documentation maintained in the personnel files. The University could accomplish this by requiring that a second employee verify all payroll data entered in the payroll system.

- Require that the renewal of annual contracts is documented per university and Arizona Board of Regents' policies, and that all pay data documentation is retained.

- 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, and monitor the assignment of payroll processing user roles to ensure that approval authority is limited to the appropriate users.

- Require that departments implement policies and procedures to ensure that leave requests for exempt employees are reviewed and monitored.

- Continue to monitor salary increases and additional pay to ensure their propriety.

- Monitor overpayment listings to ensure accuracy, completeness, and timely collection of overpayments as well as to identify potential internal control weaknesses.

- Adhere to university-established policy by centrally maintaining employee personnel records.

A similar finding was noted in the previous year.

09-02
The University should strengthen controls over access and change management, and update its disaster recovery plan for its computer information systems

Criteria: The University should have effective computer system access controls to prevent and detect unauthorized use, modification of programs and data, and misuse of sensitive or confidential information. Also, to help ensure that its information systems function as designed, it is essential that program changes to the systems are properly documented, authorized, tested, and approved before modifications are made. Further, no one employee should be responsible for the entire program change process. In addition, the University should have an up-to-date disaster recovery contingency plan in place to provide for continuity of operations and to ensure that electronic data files are not lost in the event of a system or equipment failure or other system interruption.

Condition and context: While testing internal controls for the University's general ledger, human resources and payroll, and student information systems, auditors noted the following:

General ledger system

- The University did not always remove users' access rights after the user terminated, retired, or transferred to a different department. For example, for 5 of 32 employees selected for test work, the University did not remove access rights when an employee was transferred to another department. In addition, based on a listing of all employees terminated in fiscal year 2009, 18 employees had general ledger access after their termination dates.

- The University did not effectively separate responsibilities for program changes since one employee was responsible for making program changes, there were no independent reviews of the changes, and the same employee requested that program changes be moved into production. Further, no monitoring of general ledger database changes was performed.

- The University's disaster recovery plan was inadequate since it did not address all the necessary elements to continue operations in the event of a disaster and it had not been updated or tested since April 2006.

Human resources and payroll, and student information systems

- The University did not have written policies and procedures in place to ensure employees were assigned the appropriate level of system access that was compatible with the employees' job responsibilities. Auditors noted 5 of 77 employees selected for test work had conflicting roles assigned to them.

- The University did not always review access logs to determine if user accounts had been inactive for an extended period of time. Additionally, the University did not always remove access rights after a user terminated, retired, or transferred to a different department. Auditors noted 17 employees who had access to the system after their termination dates.

- The University did not ensure that program changes to the systems were properly documented, authorized, tested, and approved prior to being implemented. For example, auditors noted 13 of 25 program changes selected for test work lacked adequate supporting documentation.

- The University did not have a written disaster recovery contingency plan.

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 monitored. Also, erroneous program changes could result in the systems not functioning as designed and materially affecting financial statement information. Additionally, the University could experience the loss of computer operations in the event of a system or equipment failure or other interruption since the University lacked an adequate disaster recovery contingency plan. This finding is a material weakness in internal control over financial reporting.

Cause: The University did not devote resources to adequately monitor employee system access rights, control program changes, or maintain a disaster recovery contingency plan.

Recommendation: To help strengthen controls over system access, program change management, and disaster recovery, the University should perform the following:

General ledger system

- Review system access rights on a continual basis to ensure that access rights are removed or changed when employees terminate, retire, or transfer to a different department within the University.

- Train additional employees to help with program changes for the general ledger system. These employees can help develop and test program changes and review migration requests for propriety before they are submitted to the Technical Operations Support group for implementation.

- Update its disaster recovery contingency plan to develop procedures for backup tape recovery, application disaster recovery, and provide regular updates and notices regarding disk storage requirements.

Human resources and payroll, and student information systems

- Develop and implement procedures to monitor user access rights and ensure that employees do not have access with conflicting responsibilities assigned to them.

- Review system access rights on a continual basis to ensure that access rights are removed or changed when employees terminate, retire, or transfer to a different department within the University.

- Monitor all program changes to ensure that all changes are documented, authorized, tested, reviewed, and approved before implementation.

- Regularly review its hosting service contracts and update its disaster recovery contingency plan to ensure that controls identified as necessary to complement the controls at the service organization are implemented.

A similar finding was noted in the previous year.

09-03
The University needs to perform regular security risk assessments for its Web-based applications used to grant access to its computer systems

Criteria: The University should perform regular security risk assessments to prevent and detect unauthorized use and misuse of sensitive or confidential information.

Condition and context: As reported in the Auditor General's performance audit report, *Arizona‘s Universities—Information Technology Security*, Web-based applications were vulnerable because of a combination of weaknesses that could allow unauthorized access to the University's computer systems and the sensitive financial and personal information they contain. While the University has taken corrective action to address the specific Web-based vulnerabilities identified in our 2008 performance audit report, the University did not provide sufficient evidence to support that security risk assessments were performed during fiscal year 2009.

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

Cause: The University did not devote resources to regularly perform security risk assessments for its Web-based applications.

Recommendation: The University should continue its efforts for ensuring its systems and the financial and sensitive information they contain are protected from unauthorized access and use. Additionally, these efforts should specifically include performing security risk assessments of the Web-based portions of the human resources and payroll, and student information systems. The University should also develop procedures to conduct security reviews on a regular basis to assess whether security controls are functioning effectively, and to help ensure problems found are corrected.

A similar finding was noted in the previous year.

ASU Arizona State University

FINANCIAL SERVICES

PO Box 877505
Tempe, AZ 85287-7505

(480) 965-7228
Fax: (480) 727-9922

January 12, 2010

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 recommendations, and related corrective action plans and current status, in conjunction with the financial audit for the year ended June 30, 2009, 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,

Gerald E. Snyder
Senior Advisor to the Executive Vice President,
Treasurer, and Chief Financial Officer

Enclosure

c: Morgan R. Olsen, Executive Vice President, Treasurer and CFO
Adrian Sannier, University Technology Officer and Vice President
Joanne Wamsley, Senior Associate Vice President for Finance and Deputy Treasurer
Kevin Salcido, Interim Associate Vice President/Chief Human Resource Officer

1/12/10

Arizona State University

Responses to the Recommendations,
And Related Corrective Actions Plans and Current Status,
In Conjunction with the Financial Audit for the Year Ended June 30, 2009
(Responded to in order as presented in the Auditor General's Report)

Finding 09-01: The University should strengthen controls over payroll expenses.

In regard to the recommendations of the auditors in finding 09-01, ASU's response and current status are as follows:

- **Establish a comprehensive set of policies and procedures for processing, monitoring, and verifying payroll expenses**.

  This recommendation is presently scheduled to be completed during fiscal year 2010.

  The University has enhanced existing policies and is in the process of creating new policies and procedures related to processing, monitoring and verifying payroll expenses.

  The following have been completed:

  - Updates to Org Manager Responsibilities policy (FIN 203) to include specific reference to verifying salary and/or wage expenses by employee.
  - Development of business process guide to assist departments in payroll reconciliations.
  - Development of certification process to ensure that payroll reconciliations are completed.
  - Updates to Overpayment policy (SPP 405-02) which outlines the process to be followed if an overpayment has been detected.

  The following enhancements are currently in process:

  - Development of a Payroll Time Reporting policy (SPP 405-03) which addresses guidelines for reporting of time as well as responsibilities of employees, supervisors and department time administrators. This University wide policy replaces various departmental time reporting policies.
  - Development of time reporting guidelines which summarizes the responsibilities outlined in SPP 405-03.
  - Development of business manager web site to house all policies and procedures for payroll and payroll related processes centrally.
  - Periodic reviews by Financial Services of detailed departmental payroll reconciliations.

- **Ensure that all departments prepare monthly reconciliations of payroll expenses for individual employees to the terms of their employment agreement. .**

  This recommendation has been implemented.

  The University agrees that at the time of the audit sample review (consisting of 81 departments), 41 of the 56 departments were doing a high level review of payroll expenses, and 15 departments were doing no review or only a very limited review. The other 25 departments sampled were doing detailed reconciliations by position, as prescribed by University policy. Hence, 80 percent of the departments were doing at least high level reconciliations. Even with a high level review, most material payroll over or under payments would had been found. University policy, however, requires a detailed review of payroll expense for each employee, to capture all over or under payments. During late summer 2009, all ASU departments were required to perform a detailed reconciliation of all fiscal year 2009 payroll expenses by employee, as certified to Financial Services by the highest level business administrator in each dean's and vice president's office in order to provide assurance for fiscal year 2009 that any over or under payments had been identified. Although some additional small overpayments were identified, no significant payroll issues were uncovered as a result of this comprehensive review.

  ASU is continuing with this annual certification process to ensure that detailed payroll reconciliations are timely performed during the year, resulting in completion of this recommendation. Additionally, as a further enhancement, ASU is automating a significant portion of the detailed, by-employee reconciliation process, which will reduce the time required to do the reconciliations and make the process easier for the departments. This new, more automated process, is presently in pilot mode for a limited number of departments with an anticipated roll out to all departments in fiscal year 2010.

  Effective with fiscal year 2010, Financial Services also is performing periodic reviews during the year of detailed payroll reconciliations performed by departments to insure that all required policies/procedures in this area are being timely followed.

- **Improve controls over employee payroll to ensure that pay data reflected in the payroll system is supported by the contract, offer letter, or other official documentation maintained in the personnel files. This could be accomplished by requiring that a second employee verify all payroll data entered in the payroll system.**

  This recommendation has been implemented.

  The Data Management Section of HR now requires supporting documentation of personnel transactions to verify submitted information.

  The Payroll Department now requires copies of source documents with appropriate signatures for processing of payroll corrections and additional pay requests. As part of the regular payroll reconciliation process, departments now confirm that employee paychecks are consistent with the approved/authorized hours as recorded, as well as verifying that any additions/corrections processed have been captured to ensure the accuracy of the paycheck.

- **Require that the renewal of annual contracts is documented per university and Arizona Board of Regents policies, and that all pay data documentation is retained.**

  This recommendation has been implemented.

  Notices of Appointment, through a new automated process, were completed for FY 2010. There are planned enhancements to this process for FY 2011.

- **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, and monitor the assignment of payroll processing user roles to ensure that approval authority is limited to the appropriate users.**

  Part of this recommendation has been implemented, with the remaining portion scheduled to be completed during FY 2010.

  Policy SPP 405-03, Payroll Time Reporting, is being established in order to formalize and clarify University practices that ensure time records are contemporary and accurately reported.

  Time Recording Guidelines, which summarize responsibilities of employees, supervisors and Department Time Administrators, also are being developed and implemented in FY 2010.

  The Assistant Director of Payroll reviews a monthly security report of access roles for payroll processing users, to ensure that these roles are limited to appropriate users within the payroll unit of the Office of Human Resources, and initiates changes where appropriate. In addition, ASU has developed and implemented a process to terminate access when employees transfer to a different department.

- **Require that departments implement policies and procedures to ensure that leave requests for exempt employees are reviewed and monitored.**

  This recommendation is scheduled to be completed during fiscal year 2010.

  SPP 702-01, Vacation Leave, is being revised to include University wide vacation reporting guidelines for exempt staff. Time Reporting Guidelines to summarize responsibilities of each party (SPP 405-03) also are being developed as noted above.

- **Continue to monitor salary increases and additional pay to ensure their propriety.**

  This recommendation has been implemented.

  Salary increases are monitored through the approval process guidelines which have been provided by the Provost Office (academic areas) and Executive Vice President, Treasurer, and CFO (business operations and President's area). Salary increases are verified by the required receipt of appropriate approval prior to data entry by the HR Data Management staff, implemented in FY 2009.

  The process for additional pay is as follows: Departments are required to get the appropriate written approvals at the departmental level; then send the online pay change to the Office of Human Resources – Payroll Section for processing. The Payroll department reviews the documentation to ensure that the appropriate approvals have been received prior to data entry.

- **Monitor overpayment listings to ensure accuracy, completeness, and timely collection of overpayments as well as to identify potential internal control weaknesses.**

  This recommendation has been implemented.

  The Office of Human Resources – Payroll Section completes a monthly review of the overpayment log to look for potential internal control weaknesses and related trends, and to ensure that all overpayments are rectified, implemented in FY 2009.

  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 letters for repayment. If there is no response from the former employee, the case is then referred to ASU's internal collections department. The internal collections 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 outside collections agencies and reported to credit bureaus.

- **Adhere to university-established policy by centrally maintaining employee personnel records.**

  This recommendation is scheduled to be completed during FY 2010.

  ASU has directed that departments provide documentation to a central location within the university of personnel actions since the PeopleSoft Human Resources Information System implementation date (7/1/2007) for both the initial job record creation and job record changes. Communication of the importance of centrally housing the personnel files, in compliance with current policy SPP 1101: Personnel Records also was reinforced for all payroll actions on a going forward basis. Policy Clarification already has been implemented, with the planned record centralization completion scheduled for FY 2010.

Finding 09-02: The University should strengthen controls over access and change management, and update its disaster recovery plan for its computer information systems.

ASU's response and current status are as follows for each of its enterprise applications:

General ledger System

- **Review system access rights on a continual basis to ensure that access rights are removed or changed when employees terminate, retire, or transfer to a difference department within the University.**

  This recommendation has been implemented.

  The University implemented enhanced procedures to remove or change access rights to the Advantage general ledger when employees terminate, retire or transfer to a different department within the University. The enhanced procedures include a review of a daily report that compares mainframe access to Advantage access and identifies exceptions, a more frequent review of the employee status code of all staff with Advantage access and the review of all employees with Advantage access who have been identified as transfers within the PeopleSoft transfer process. These reviews are done by the Advantage Helpline and access rights are changed or terminated where appropriate.

- **Train additional employees to help with program changes for the general ledger system. These employees can help develop and test program changes and review migration requests for propriety before they are submitted to the Technical Operations Support group for implementation**.

  This recommendation has been implemented.

  The University has trained additional developers to help with program changes for the general ledger system. This includes testing and reviewing programming changes.

- **Update its disaster recovery contingency plan to develop procedures for backup tape recovery, application disaster recovery, and provide regular updates and notices regarding disk storage requirements.**

  This recommendation has been implemented.

The University has updated its disaster recovery contingency plan. ASU now hosts its financial accounting system with ADOA and has business continuity procedures for the purposes of disaster recovery. ASU's hosting partner, the Arizona Department of Administration (ADOA), is jointly responsible with ASU for tape backup and recovery, disk backup and recovery, and application disaster recovery. ASU monitors and provides regular updates and notices regarding disk storage requirement as needed.

Human resources and payroll and student information systems

- **Develop and implement procedures to monitor user access rights and ensure that employees do not have access with conflicting responsibilities assigned to them.**

  This recommendation has been implemented.

  The University has procedures to monitor user access rights. Audit reports are generated for PeopleSoft data trustees to review on a monthly basis. These reports show who has access to the roles they administer. A Data Trustee policy has been published that emphasizes the importance of segregation of duties, and training sessions for the data trustees have been held. Access assignments for the individuals noted in the finding have been reviewed and appropriate action taken.

- **Review system access rights on a continual basis to ensure that access rights are removed or changed when employees terminate, retire, or transfer to a different department with the university.**

  This recommendation has been implemented.

  The University developed and implemented a process to remove PeopleSoft roles automatically for terminated employees in fiscal year 2008. This process only ran periodically in fiscal year 2009. Beginning the first quarter of fiscal year 2010, this process is run daily. In the second half of fiscal year 2009, ASU developed and implemented a process to terminate access when employees transfer to a different department. Other administrative access for terminated employees is automatically revoked based on their change of affiliation status. Retirees are treated as employee terminations but are granted a courtesy affiliate status which enables them to retain basic services such as email.

- **Monitor all program changes to ensure that all changes are documented, authorized, tested, reviewed, and approved before implementation**.

  This recommendation has been implemented.

  The University now monitors all program changes to ensure they are documented, authorized, tested, reviewed, and approved before implementation. The 13 out of 25 program changes noted in the audit that lacked adequate supporting documentation had all been submitted prior to the University implementing a more formalized procedure in the third quarter of FY 2009. All program changes now are submitted through an internal tracking system and require proof of the program change requests, functional specifications, test plan(s), technical review, and functional approval. A final check is verified by the PeopleSoft Systems team before submitting a request to make the change in Production. These procedures are documented in the PeopleSoft Systems Reference Guide

- **Regularly review its hosting service contracts and update its disaster recovery contingency plan to ensure that controls identified as necessary to complement the controls at the service organization are implemented**.

  This recommendation has been implemented.

  The University now regularly reviews its PeopleSoft hosting service contracts and disaster recovery contingency plans annually and updates its disaster recovery contingency plan to ensure that controls identified as necessary to complement the controls at the service organization are implemented.

Finding 09-03: The University needs to perform regular security risk assessments for its Web-based applications used to grant access to its computer systems.

- **The University should continue its efforts for ensuring its systems and the financial and sensitive information they contain are protected from unauthorized access and use. Additionally, these efforts should specifically include performing security risk assessments of the Web-based portions of the human resources and payroll and student information systems. The University should also develop procedures to conduct security reviews on a regular basis, to assess whether security controls are functioning effectively, and to ensure problems found are corrected.**

  This recommendation has been implemented.

  The University continues its efforts to ensure that systems are protected from unauthorized access and use. The University has a standard for performing security assessments for high criticality web applications, and the PeopleSoft Human Resources Information and Student Information systems. In FY 2010, ASU solidified an arrangement with a third party company to begin regular security assessments for the hosted PeopleSoft systems, which will occur twice per year. The initial security scan under this arrangement was completed in FY 2010 and another scan will be scheduled before the end of FY 2010.