Financial Statement Findings and State Responses
(Reformatted from FY 2009 Single Audit Report)

09-01
The Department of Administration should prepare accurate financial statements in a timely manner

Finding

Criteria: The Department of Administration should issue accurate and timely financial statements for the State to satisfy the audit requirements imposed by federal and state laws and regulations, grant contracts, and long-term debt agreements.

Condition and context: The Director of the Department is responsible for establishing and maintaining the State's accounting systems and preparing accurate and timely financial reports, including the State's Comprehensive Annual Financial Report (CAFR). In accordance with Arizona Revised Statutes (A.R.S.) §41-703, the Director has the authority to promulgate rules, regulations, and procedures to carry out his responsibilities. Further, A.R.S. §35-131(I), requires state agencies and other organizations included in the State's reporting entity to submit all necessary financial information to the Department in accordance with its policies and procedures. However, those statutes did not include provisions to enforce compliance, and as a result, state agencies did not always comply with the established deadlines. For example, of the 16 state agencies that had a November 30, 2009, deadline to submit their audited financial statements, only 8 met this deadline, and 1 did not submit its audited financial statements until February 3, 2010.

Effect: Since various state agencies did not comply with state statutes or department rules and regulations, the State did not issue its CAFR by its December 31, 2009, deadline. Delays in financial reporting may result in rating agencies lowering the State's ratings for bonds and certificates of participation. Also, the State's Single Audit Reporting Package will be issued late (see finding 09-101), which could result in a loss of federal funding. This finding is a material weakness in internal control over financial reporting.

Cause: State statutes do not provide the Director of the Department with enforcement power to ensure that state agencies comply with department rules, regulations, and procedures for financial reporting.

Recommendation: To help ensure that the Department receives financial information necessary for timely issuance of the State's CAFR, the Department should:

- Seek the authority to enforce rules, regulations, and procedures over financial reporting.
- Establish enforcement actions for agencies' failure to submit such information by the required deadlines.

This finding was similar to a prior-year finding.

Agency Response: Concur

Contact person: Clark Partridge, State Comptroller, (602) 542-5405
Anticipated completion date: June 2012

Agency Corrective Action Plan: Timeliness is one of the fundamental thresholds of financial reporting and the timely issuance of the CAFR is vital to other reporting requirements and deadlines. A.R.S. §35-131 clearly requires State agencies and other organizations that are part of the State's reporting entity to submit all necessary financial statements and other information in accordance with the policies and procedures of the Arizona Department of Administration, General Accounting Office. This includes adherence to established time frames and deadlines. However, there are no specific provisions in the law for actions that may be taken to enforce such compliance. We can continue to explore potential options for enforcement actions and will continue to work with State agencies to effectively resolve the issue of timely submission of financial information.

Financial Statement Findings and State Responses
(Reformatted from FY 2009 Single Audit Report)

09-02
The Department of Administration should establish fraud prevention and detection programs

Finding

Criteria: The State of Arizona should have a strong system of internal control, including a state-wide antifraud program or other methods to help reduce the possibility of fraud and promote ethical behavior.

Condition and context: The Director of the Department of Administration is responsible for establishing and maintaining adequate written policies and procedures to ensure overall operational efficiency and effectiveness and compliance with laws and regulations. Individual state agencies may have controls designated to mitigate specific risks of fraud. However, the Department had not established a state-wide program that addressed fraud risk.

Effect: The lack of a comprehensive antifraud program for the State could result in fraud and possible misuse of state monies. Additionally, financial statement misstatements due to fraud could occur. This finding is a significant deficiency in internal control over financial reporting.

Cause: The Department has not completed its state-wide antifraud program because of inadequate resources.

Recommendation: To strengthen state-wide internal controls to allow management to anticipate and react to internal and external fraud risks, the Department should establish the following:

- A state-wide program designed to prevent, deter, and detect fraud and promote a culture of honesty and ethical behavior.
- A communication channel for citizens and employees to report suspected unethical behavior, fraud, or code of conduct violations.

This finding was similar to a prior-year finding.

Agency Response: Concur

Contact person: Clark Partridge, State Comptroller, (602) 542-5405
Anticipated completion date: June 2009

Agency Corrective Action Plan: A policy was issued on June 12, 2009. A summary of the policy follows:

State financial policy does not tolerate any type of fraud or theft and all instances must be reported to either GAO, the Auditor General, or the Attorney General. The GAO has established the e-mail address reportfraud@azdoa.gov to facilitate this reporting. It is management's responsibility to control waste and abuse. The GAO is available for consultation regarding internal controls and opportunities to reduce waste and abuse. The State's policy is to promote consistent, legal, and ethical organizational behavior by:

- Assigning responsibility for reporting fraud, theft, waste, or abuse; and
- Providing guidelines to conduct investigations of suspected fraudulent behavior.

Although we consider this issue to be fully corrected, we will continue to evaluate internal controls and provide additional policy and guidance as appropriate. We have also implemented a periodic survey of internal controls to be submitted by the agencies.

09-03
The Department of Administration should strengthen controls over the Human Resource Information Solution (HRIS) account management

Finding
Criteria: Account management controls cover the request, approval, establishment, suspension, and termination of user accounts. These controls are vital to system security, and therefore, the Department of Administration should have adequate policies and procedures for account management over its HRIS system.

Condition and context: While obtaining an understanding of the Department's internal controls over HRIS account management and testing those controls, auditors noted the following deficiencies:

- The Department did not have written comprehensive policies for account management of operating system accounts and database accounts.
- Activity logs used to track user access to the application and changes made to data, including salary information and number of hours worked, were not regularly monitored. Additionally, there were no controls to prevent HRIS administrative users from altering or deleting the data in these logs.
- The Department manually maintained a spreadsheet of all HRIS users. However, this spreadsheet was not reconciled to a system-generated listing of users.
- Employees who received a user account for HRIS were required to complete training for the job roles they had been granted access for. However, seven of the ten employees tested had not completed the general prerequisite training. Additionally, one of these seven was also missing a portion of the specific training directly related to his job role.
- An agency user was given access that did not allow for proper separation of responsibilities, and there were no written explanations of compensating controls from the user's agency.

Effect: Without effective account management controls, security over the HRIS system is weakened since the Department cannot ensure that the approval, establishment, suspension, and termination of accounts are performed properly and in accordance with management requirements. This finding is a significant deficiency in internal control over financial reporting.

Cause: The Department did not establish or enforce sufficient written policies and procedures related to account management. Additionally, due to limited resources, the Department did not feel it was necessary to monitor the activity logs or reconcile the manual spreadsheet of users to a system-generated listing of users.

Recommendation: To help strengthen controls over account management, the Department should perform the following:

- Develop written account management policies for operating system and database accounts.
- Regularly review activity logs that monitor user access and changes made to data and investigate any unusual activity. Additionally, administrative users should have read-only access to these logs.
- Reconcile the manual spreadsheet of users to the system-generated listing of users.
- Develop a process to ensure compliance with the Department's own internal policy related to granting HRIS user accounts.
- Retain all supporting documentation for granting user access.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Jody Lauer, HRIS Manager, (602) 542-4282
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: In regard to the recommendations of the auditors, HRIS's response and current status are as follows:

- Develop written account management policies for operating system and database accounts. HRIS concurs and is in the process of documenting the policy for operating system and database accounts. The only employees with access to these types of accounts are HRIS system administrators and Database Administrators. Anticipated completion date: June 30, 2010.
- Regularly review activity logs that monitor user access and changes made to data to ensure compliance. Additionally, administrative users should have read-only access to these logs. HRIS keeps track of changes made by HRIS Table Maintenance personnel via the HRIS audit tables. These tables have been reviewed when there is a question as to who made a change or what information was changed to certain critical HRIS tables. There is a separation of duty regarding these tables. HRIS Table Maintenance personnel key information into HRIS and this triggers the updates to the audit tables. They do not have direct access to the audit tables. The database administrators (two) do have access to the audit tables, but do not perform the updates that trigger the updates to the audit tables. Database administrators must have access to all tables as a requirement of their job responsibilities. HRIS will begin monitoring these HRIS audit tables to validate changes against Change Control Board (CCB) approved items.
- Reconcile the manual spreadsheet of users to the system-generated listing of users. HRIS concurs with this finding. The HRIS security team has since reconciled the manual spreadsheet to a system-generated listing of users upon this finding. This procedure will also be performed on a quarterly basis. Estimated completion of reconciliation: Completed and on-going quarterly.
- Develop a process to ensure compliance with the Department's own internal policy related to granting HRIS user accounts. HRIS has a documented process for granting HRIS user accounts. To ensure this process is followed, each quarter HRIS will perform a reconciliation process validating the system-generated listing of HRIS users and their security class settings to the spreadsheet maintained by the HRIS security officers. In addition, all HRIS training (prerequisite and job role specific) exams are now taken in the Learning Management System (LMS). The system now enforces all prerequisite courses must be taken and the exam passed before a user can take job role specific training. The LMS automatically updates employees training history records in Y.E.S., allowing the HRIS security administrators to view training history and verify all exams have been passed before granting access into HRIS.
- Retain all supporting documentation for granting user access. HRIS does retain all supporting documentation for granting user access. If it is discovered that documentation is missing during our quarterly reconciliation process, HRIS will require the requesting agency to provide the missing documentation; otherwise, access to HRIS will be removed until such documentation is provided.

09-04
The Department of Administration should improve controls over HRIS system changes

Finding
Criteria: All system changes should be monitored to ensure that changes are authorized and adhere to established system change policies.

Condition and context: While obtaining an understanding of the Department's internal controls over HRIS system changes, auditors noted the following deficiencies:

- The system-generated log used to track operating system changes could be modified by administrative users. Additionally, Tripwire reports were used to monitor compliance with system change policies; however, management was not able to identify noncompliance with its policies and procedures, including separation of responsibilities violations, by reviewing these reports.
- There was no system-generated log to record changes made directly to the database.

Effect: Inadequate program change management could lead to unauthorized changes, incorrect changes, or ineffective changes, and could result in the system not functioning as designed. This finding is a significant deficiency in internal control over financial reporting.

Cause: Due to limited resources, the Department did not devote resources to regularly monitor operating system change logs or develop a change log for changes made directly to the database.

Recommendation: To help strengthen controls over changes to the HRIS system, the Department should:

- Ensure the system-generated log used to track operating system changes cannot be altered by administrative users and the Tripwire reports are reviewed on a weekly or monthly basis to ensure changes were authorized and followed system change policies.
- Develop a system-generated log of changes made directly to the HRIS database.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Jody Lauer, HRIS Manager, (602) 542-4282
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: In regard to the recommendations of the auditors, HRIS's response and current status are as follows:

- Ensure the system-generated log used to track operating system changes cannot be altered by administrative users and the Tripwire reports are reviewed on a weekly or monthly basis to ensure compliance. HRIS system administrators have root access to the system and must have this in order to perform their job duties. Root access does have the capability of modifying anything on the UNIX box as it is the "power user" of the system. This is why we have implemented the Tripwire reports as it does the reporting on operating system changes. Tripwire administration is handled by ISD-AIS, not the HRIS system administrators. Any policy changes to Tripwire reporting requirements must be approved by HRIS management and ISD-AIS security and are implemented by ISD-AIS, not HRIS. All commands executed at the UNIX command prompt are stored in UNIX shell history (last 10,000 commands) for each user. In addition, this shell history is backed up nightly and stored off-site. Tripwire reports are reviewed daily by HRIS management. Tripwire changes are promoted weekly and commented as to where the change originated (CCB for HRIS programs or Change Control Form for system administration items). They are reviewed to ensure compliance with HRIS change management procedures. As noted above, it does not show separation of duties violations, but reviewing the shell history of users would determine what commands were executed by an individual.
- Develop a system-generated log of changes made directly to the HRIS database. DB2 has logging enabled that tracks all changes to the database, regardless if they were made directly to the database or using Lawson programs. This logging is used for database restores and recovery and is not editable by database or system administrators. However, this functionality is not used to audit user activity.

09-05
The Department of Administration's State Procurement Office (SPO) should ensure the Procurement System Administrator does not have access to data

Finding
Criteria: According to industry standards, proper audit trails should be maintained so that changes to databases and their contents can be monitored.

Condition and context: The Department of Administration's State Procurement Office uses an automated procurement system, SPIRIT, which was developed to increase the efficiency of procuring goods and services and to improve customer service. The SPIRIT system's Web interface replaces the previous paper-based procurement process. The SPIRIT System Administrator had access to data on the SPIRIT system and could revise vendor bids at the vendor's request. However, to document these changes, the Office only maintained a manual log.

Effect: There is a possibility of misuse or fraud if changes are made to the system without adequate supporting documentation. In addition, vendor bids could be changed with no written documentation from the vendors. This finding is a significant deficiency in internal control over financial reporting.

Cause: The SPO does not plan to install an electronic logging function to monitor changes made to data in the database since the SPIRIT system has been replaced with a new automated procurement system**.**

Recommendation: To help ensure proper oversight and documentation of revised vendor bid submissions, the SPO should do one or more of the following:

- Request that the Information Systems Division prevent the System Administrator from having the ability to change system data.
- Enable the logging function in the new procurement system to track administrator user changes through an automated log, journal, time stamp, or other method that would document the change.
- Have the vendor resubmit the bid or add an amendment to the original document.
- Require vendors to submit signed, prenumbered forms that list the changes made and the reasons for them.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Jean Clark, State Procurement Administrator, (602) 542-5508
Anticipated completion date: September 1, 2009

Agency Corrective Action Plan: The State Procurement Office acknowledges the 2008 and 2009 Audit Findings in regard to SPIRIT. In response to these audit findings and SPIRIT's limitations and age, the State Procurement Office replaced SPIRIT on September 1, 2009. Further, with the implementation of the new e-procurement system, ProcureAZ each of these audit findings have been addressed.

09-06
The Department of Administration's SPO needs to have more than one person capable of maintaining the procurement system's Web application

Finding

Criteria: Industry standards state that organizations should minimize overdependence on key employees through documentation, knowledge sharing, succession planning, and staff backup.

Condition and context: The development, updating, and maintenance of the SPIRIT system's Web application is solely performed by one person employed by a third-party contractor.

Effect: If the individual leaves the third-party contractor, neither the contractor nor the SPO would have employees with the knowledge to effectively update and maintain the SPIRIT system. This finding is a significant deficiency in internal control over financial reporting.

Cause: The SPO did not develop a contingency, cross-training, or knowledge-sharing plan to ensure the continued maintenance and support of the SPIRIT system since the SPIRIT system has been replaced by a new procurement system.

Recommendation: To help ensure continued system maintenance, the SPO should develop a contingency plan for its new procurement system. This could entail requiring the third-party contractor to employ other persons with the knowledge necessary to maintain the system, requiring the contractor to maintain detailed documentation regarding the system's development and operation so that others could maintain the system, or training in-house employees to maintain the system.

This finding was similar to a prior-year finding.

Agency Response: Concur

Contact person: Jean Clark, State Procurement Administrator, (602) 542-5508
Anticipated completion date: September 1, 2009

Agency Corrective Action Plan: The State Procurement Office acknowledges the 2008 and 2009 Audit Findings in regard to SPIRIT. In response to these audit findings and SPIRIT's limitations and age, the State Procurement Office replaced SPIRIT on September 1, 2009. Further, with the implementation of the new e-procurement system, ProcureAZ each of these audit findings have been addressed.

09-07
The Department of Administration's Information Systems Division (ISD) should strengthen access controls over its procurement system

Finding

Criteria: System and logical access controls help ensure that only authorized users have access to the SPIRIT system and are necessary to protect the system and data from unauthorized use, damage, loss, modification, or disclosure. Access controls should prohibit users from having access to functions not required to perform their jobs.

Condition and context: The application developer was able to modify files affecting the SPIRIT system design and functionality.

Effect: Inadequate access controls may allow users to read, change, or delete data without specific authorization. The application developer or other users could change files affecting the procurement design and functionality, and those changes could be applied to the system without approval. This finding is a significant deficiency in internal control over financial reporting.

Cause: The ISD has policies and procedures to control access granted to application developers. However, administrative access control lists were not reviewed after changes were made to the system or on a regular basis.

Recommendation: To help prevent and detect unauthorized use, damage, loss, or modification of programs and data, the ISD should restrict the application developer's access to files affecting the SPIRIT system design and functionality. Further, an ISD employee should review access control lists on a monthly basis and investigate any unusual activity.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Jean Clark, State Procurement Administrator, (602) 542-5508
Anticipated completion date: September 1, 2009

Agency Corrective Action Plan: The State Procurement Office acknowledges the 2008 and 2009 Audit Findings in regard to SPIRIT. In response to these audit findings and SPIRIT's limitations and age, the State Procurement Office replaced SPIRIT on September 1, 2009. Further, with the implementation of the new e-procurement system, ProcureAZ each of these audit findings have been addressed.

09-08
The Department of Administration's ISD should strengthen controls over the SPIRIT system's software updates

Finding
Criteria: The Department of Administration's ISD should ensure all servers hosting the SPIRIT system receive the appropriate software and software updates.

Condition and context: The current software did not provide adequate security protection for the SPIRIT servers. Because of the nature of this finding, the specific details of the finding were verbally communicated to those officials directly responsible for implementing corrective action.

Effect: The potential for data loss and system corruption and the cost to restore system network integrity could be detrimental to the Department. This finding is a significant deficiency in internal control over financial reporting.

Cause: Lack of personnel has prevented the ISD from testing and implementing the necessary software and updates. Further, since the system is being replaced, no effort will be made to correct the problem.

Recommendation: Since the SPIRIT system is being replaced, it is imperative that the ISD include the necessary security software and software updates on the new procurement system.

Agency Response: Concur
Contact person: Lori Boak, Information Services Division, (602) 542-1422
Anticipated completion date: September 1, 2009

Agency Corrective Action Plan: The new procurement system is hosted at CGI, and the Periscope/CGI teams are currently auditing the system. The SPIRIT archive is the only portion of the system that is being hosted at the ADOA Data Center. The archive is using a Windows Server and is configured for automatic updates from Microsoft on a weekly basis to ensure current patches, etc., are applied.

09-09
The Department of Administration's ISD should strengthen controls over access to the SPIRIT system's Web site

Finding
Criteria: The Department of Administration's ISD should ensure the SPIRIT system is protected from unauthorized access.

Condition and context: The SPIRIT system's Web site was vulnerable to attacks or unauthorized access. Because of the nature of this finding, the specific details of the finding were verbally communicated to those officials directly responsible for implementing corrective action.

Effect: Possible outcomes of Web site attacks include unauthorized access to confidential data or disruption of service. This finding is a significant deficiency in internal control over financial reporting.

Cause: SPIRIT system administrators were unaware of the problem and have not made any modifications this year since the SPIRIT system is being replaced.

Recommendation: For the Department's new procurement system, the ISD should ensure that information is protected from attack, and the ISD should ensure that the new system performs input edits and checks to determine that information received complies with acceptable and expected formats.

Agency Response: Concur
Contact person: Lori Boak, Information Services Division, (602) 542-1422
Anticipated completion date: September 1, 2009

Agency Corrective Action Plan: The new procurement system is hosted at CGI, and the Periscope/CGI teams are currently auditing the system. The SPIRIT archive is the only portion of the system that is being hosted at the ADOA Data Center. The archive system is behind a Profense Web Application firewall. This provides defenses against the OWASP top ten vulnerabilities, including validation of user input.

09-10
The Industrial Commission of Arizona needs to strengthen controls over financial reporting

Finding
Criteria: The State must issue timely financial statements to satisfy the audit requirements imposed by federal laws, state statutes and regulations, grant contracts, and long-term debt covenants. Additionally, financial reporting responsibilities should be adequately separated so that several employees can perform these functions.

Condition and context: To help ensure that the State's financial statements are prepared and issued in a timely manner, the Department of Administration's General Accounting Office (GAO) had established timelines for the individual state agencies to submit required financial information to it for inclusion in the state-wide financial statements. Then, the Commission's management was responsible for preparing complete and accurate financial statements for the Commission's Special Fund and submitting them to the GAO in a timely manner. However, the Commission did not meet the GAO reporting timelines. The Commission submitted preliminary financial

information to the GAO on November 11, 2009, approximately 7 weeks late, and its final financial information on March 12, 2010, approximately 4 months late. Further, the Commission was dependent on a single employee who possessed all of the critical knowledge necessary to make the necessary adjusting entries and compile the financial statements.

Effect: Submission of late financial information could result in missed reporting deadlines, including the OMB Circular A-133 reporting deadline, and a loss of federal funding for the State as a whole. Also, in the event that the employee leaves the Commission or is unable to perform his responsibilities, other employees would not possess the knowledge to compile the financial statements. This finding is a significant deficiency in internal control over financial reporting.

Cause: The delays in financial reporting resulted from the Commission's not preparing and reviewing supporting schedules and reconciliations in a timely manner, which resulted in delays in reviewing and posting transactions to the general ledger. Also, the Commission's general ledger application has limitations that prevent the Commission from posting transactions in a timely manner. Additionally, the Commission lacks resources to hire new staff, and management has not decided to train existing staff to compile financial information for the Special Fund.

Recommendation: To help ensure that accurate financial statements are prepared and issued in a timely manner, the Commission should implement the following procedures:

- Train other employees in financial reporting responsibilities.
- Develop and implement written policies and procedures that describe the necessary steps to compile the Special Fund's financial statements.
- Reconcile the financial records, and review and post all adjustments to the general ledger within 2 weeks of month-end.
- Allocate the appropriate resources, and monitor and enforce completion dates for compiling, preparing, and reviewing the financial statements and supporting schedules.
- Provide the GAO and auditors with complete and accurate financial statements, including notes and supporting schedules, by the established deadlines.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Gary Norem, Chief Financial Officer, (602) 542-5380
Anticipated completion date: July 2010

Agency Corrective Action Plan: The current Special Fund general ledger system has some limitations for posting monthly entries for the new state fiscal year (SFY) while holding the previous SFY open during the period the Auditor General completes the audit. This results in a catch-up period every year in which several months of general ledger entries need to be done within a very short period of time. In order to resolve the catch up situation, the Commission has hired a temporary accountant and is requesting critical mission approval to fill a vacant high level accounting position. With the addition of one full-time staff member dedicated to financial reporting issues, the Commission will be able to minimize the impact of the limitations of the general ledger software in future years.

The CFO will put together a time schedule for completion of the various tasks related to the financial statement preparation process. The CFO will monitor on a regular basis the work progress on the financial statements to be sure that the time lines are met. It is estimated that draft financial statements for fiscal year 2010 will be completed by October 1, 2010, and the final statements completed by November 15, 2010.

The Commission does have specific procedures for compiling the Special Fund financial statements. Two other staff members other than the CFO have considerable knowledge of the process to compile the Special Fund financial statements. However, filling the vacant higher level Accounting position and dedicating a high level accounting position to managing the compiling of the Special Fund financial statements will greatly improve the completion timeliness.

09-11
The Industrial Commission of Arizona should develop written policies and procedures for its computer operations

Finding
Criteria: Written policies and procedures provide the basic framework needed for establishing employee accountability. They serve as a reference tool for employees seeking guidance on how to handle complex or infrequent transactions and situations. Additionally, they offer guidance for controlling daily operations.

Condition and context: The Commission had not established detailed written policies and procedures over its computer operations.

Effect: Without adequate written policies and procedures, management cannot ensure that information technology controls are operating effectively. Also, it could make transitioning to a new computer system difficult and more time consuming. This finding is a significant deficiency in internal control over financial reporting.

Cause: The Commission had not established detailed written policies and procedures since it plans to replace its computer system. Therefore, it has chosen not to invest additional time or resources into an outdated system.

Recommendation: The Commission should develop and implement written policies and procedures that address the following:

- Computer operations—There should be procedures for daily operations and physical security of the computer system to help ensure that operators use the correct data, computer programs, and other resources when processing daily activity. These would help safeguard computer equipment and data against theft or misuse.
- Program changes—There should be procedures that require proper documentation and approval of program change request forms and test results, and separating responsibilities to ensure that one employee does not make, test, and implement program changes.
- Access controls—There should be procedures that address the request, approval, establishment, suspension, and termination of user accounts since this is necessary for system security.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Michael Hempel, Chief Information Officer, (602) 542-1823
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: During 2009, over 30 technical documents were on file for daily PACE operations which were maintained in a file share on the ICA file server. Also, a physical security matrix document was on file and provided to the Auditor's office as requested on April 13, 2010, for describing the physical access to the PACE system. The PACE system is maintained in a secure server room with card key controlled access.

Written procedures and change log are on file and were submitted to the Auditor's office for PACE as requested on April 13, 2010. However, it should be noted that the PACE programmer that created the database, designed the graphical user interface, and wrote the instructions to retrieve, display, and update data retired in 2008. No changes are allowed to the existing program code or database tables. Only maintenance changes required for updates to yearly reports are performed. A change log is in place if needed and any change would be authorized by the Accounting Division Manager and CIO.

The following maintenance changes are made to the WANG PACE SQL COBOL programs:

- Update of yearly tax values
- Update of fiscal and calendar year dates

Access control to the ICA computer systems is strictly controlled. The ICA staff use Microsoft Active Directory protocol, which maintains all users in a central database that controls access to workstations and applications. In 2009 the policy was put in place that HR would notify the Helpdesk via email when changes to user accounts such as termination are required. MIS helpdesk when notified by email from HR will lock out a user's Active Directory account which will terminate all access to PACE or any other Windows systems. The MIS Helpdesk staff are the only authorized personnel who are able to make Active Directory changes.

09-12
The Industrial Commission of Arizona should maintain a record of all changes to its computer system

Finding
Criteria: The Commission uses its computer system to record detailed financial transactions and generate monthly and year-end summary reports to support amounts reported in the financial statements. Therefore, it is essential that changes to the system and data be reviewed and documented.

Condition and context: When users made changes to system data, the changes were documented in the system; however, if the database administrator made changes to the system database, the changes would not be documented in the system. Additionally, although there was a log of user access, supervisors did not review these logs regularly. Finally, any changes to key computer equipment, such as firewalls, routers, or switches, were made by the chief information officer, but were not reviewed or authorized by another employee.

Effect: Unauthorized changes could be made to the system or data without detection. This finding is a significant deficiency in internal control over financial reporting.

Cause: The Commission did not have effective controls over system and data changes since it plans to replace its computer system. Therefore, it has chosen not to invest additional time or resources into an outdated system.

Recommendation: To help strengthen controls over system and data changes to its computer system, the Commission should:

- Maintain a record of all system and data changes to help monitor changes.
- Require supervisors to review user-access logs on a weekly or monthly basis.
- Have an independent employee review and authorize all major changes to computer equipment.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Michael Hempel, Chief Information Officer, (602) 542-1823
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: Per a meeting with the auditors, finding 09-12 requires that the PACE application log all system level database changes that could be made directly to the database by the PACE administrator. The PACE system was developed at a time when this was not a requirement and the system as currently in place does not have a means to log direct database administrator changes and the Commission does not have a mean to modify the code to correct this issue.

The Commission is currently developing a new Special Fund Accounting application to replace the Legacy PACE system, which is scheduled to be deployed in July 2010 to resolve this problem.

09-13
The Department of Revenue's computer access controls should continue to be strengthened

Finding
Criteria: The Department should have effective computer access controls to prevent and detect unauthorized use, damage, loss, or modification of programs and data, and misuse of sensitive or confidential information.

Condition and context: While performing test work over access controls to the Department's computerized financial information systems, auditors noted the Department did not always retain documentation to support its review and approval of users' access rights. For example, for 27 of 51 employees selected for test work, the Department was unable to provide documentation authorizing the employee's access and approval of those rights by a supervisor. Also, the Department did not remove a user's access rights after the employee separated from the Department as required by the Department's policies and procedures. In addition, the Department did not actively monitor database administrators with elevated user access privileges.

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

Cause: The Department did not commit sufficient resources to document the supervisory approval of employee access rights for reauthorizations. In addition, the Department did not have policies and procedures in place to independently monitor and review the activities of database administrators with elevated system access.

Recommendation: To help ensure the integrity of the Department's computerized financial information systems, the Department should follow its policies and procedures, which require documentation of supervisory approval on all requests for system access, and promptly terminate user access when an employee leaves employment with the Department. In addition, the Department should develop policies and procedures that require the activities of database administrators with elevated user access privileges to be independently monitored and reviewed for propriety.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Cristy Schaan, Information Security Officer, (602) 716-6758
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: Documentation of access – All 27 employees whose access rights were reviewed were employed prior to the implementation of the 2008 Systems Access Request process, which, in addition to a formal approval and review process, requires a standard level of documentation to support the authorization of users access rights. This recertification process will ensure that the Department has, and retains, the appropriate documentation for system access on all employees with system access. The recertification effort was planned for FY 2009, but because of resource constraints, the effort has been extended and is expected to be completed by September 30, 2010.

Access Removal – The Department has a process in place for removal of user access, with secondary and tertiary processes also in place to help ensure user access removal in a timely manner. All three processes are manual processes, and while we work diligently to ensure 100 percent compliance, we did not meet 100 percent compliance during this audit cycle. Moving forward, Information Security will work with business units to improve front-end processes for the removal of user access. Further, Information Security management will verify tertiary processes are complete on a monthly basis. Currently, we anticipate having this item completed by September 30, 2010.

Actively monitoring database administrators (DBAs) with elevated user access privileges – Information Security both captures and retains DBA activity but requires significant manual effort to monitor. While the Department has been working to automate this process, resource constraints have been an obstacle in accomplishing this objective. Information Security will continue efforts to configure the monitoring tool, capture activity logs and once complete begin proactive monitoring of DBA activity. Currently, we anticipate having this effort complete by June 30, 2011.

09-14
The Department of Revenue should update and test its disaster recovery plan

Finding
Criteria: For computerized information systems, it is critical for the Department to have an up-to-date contingency plan in place to provide for the 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. In addition, backup files maintaining sensitive or confidential information should be encrypted to help prevent unauthorized access to such information.

Condition and context: The Department uses computerized information systems to process and store financial and taxpayer information that is vital to its daily operations. When obtaining an understanding of the Department's internal control over its computerized tax information systems, auditors noted the Department had not completed the following:

- A risk analysis identifying and prioritizing critical applications and exposures and an assessment of the impact to the Department.
- The plan was not updated in a timely manner following the data center move in November 2008.
- The plan had not been tested since fiscal year 2007.

Further, the Department's backup files, which included sensitive or confidential information, were not adequately protected by encryption.

Effect: The Department could experience the loss of computer operations in the event of a system or equipment failure or other interruption. Further, sensitive and confidential data on the Department's backup files could be compromised. This finding is a significant deficiency in internal control over financial reporting.

Cause: The Department did not commit sufficient resources to test and update its disaster recovery plan during the fiscal year. In addition, the Department did not have adequate policies and procedures in place to help ensure backup files were adequately safeguarded.

Recommendation: To help ensure continuity of operations in the event of a major system or equipment failure, the Department should perform the following:

- A risk analysis identifying critical applications and exposures, and an assessment of the impact to the Department.
- Review, update and test the disaster plan recovery at least annually and in a timely manner following any critical events.

In addition, backup files that include sensitive or confidential information should be encrypted.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Susan Silberisen, Chief Information Officer, (602) 716-6955
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: The Information Technology division was unable to perform a complete disaster recovery test of their critical application environment due to resource constraints directly related to a large-scale data center move that was in progress through the first 2 quarters of the fiscal year. Further, during the last 2 quarters of the fiscal year there was a freeze on department expenditures. Disaster Recovery testing requires several expenditures including out-of-state travel for an employee, one-time testing charges by the data center vendor SunGard, and additional after hours AZNet charges for network redundant support.

The Department of Revenue is completing an ongoing disaster recovery plan and schedule. Currently, we anticipate having the plan completed by 2nd quarter of FY 2011, including the first test scheduled for November 2010. In addition, ADOR Information Security will evaluate our ability to budget for and implement an encryption solution for all backup tapes during FY 2011.

09-15
The Department of Revenue should continue to strengthen its procedures for processing income tax revenues

Finding
Criteria: The Department should improve procedures to further ensure that it receives and retains the tax revenues to which the State is entitled.

Condition and context: The Department is responsible for collecting all individual income taxes owed to the State. While testing procedures for income tax revenues, auditors noted additional procedures that should be performed. Because of the nature of this finding, the specific details of this finding were verbally communicated to those officials directly responsible for implementing corrective action.

Effect: The State may not receive the proper amount of individual income taxes. This finding is a significant deficiency in internal control over financial reporting.

Cause: The computer system did not have the functionality to perform the identified omitted procedures.

Recommendation: The Department should implement additional procedures necessary to compensate for the omitted procedures.

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact person: Tom MacConnel, Comptroller, (602) 716-6593
Anticipated completion date: Unknown

Agency Corrective Action Plan: The Department understands and has prioritized the continual improvement of its operations including all departmental procedures and controls and will continue to do so. Where constrained by limited resources, the Department has instituted compensating controls to help minimize risks to tax revenues.

09-16
The Department of Revenue should better protect its computer network and systems

Finding
Criteria: The Department should have effective network security controls to prevent and detect unauthorized use, damage, loss, or modification of programs and data, and misuse of sensitive or confidential information.

Condition and context: The Department is the main revenue collector for the State of Arizona, and there is a significant amount of confidential data on the Department's computerized information systems that should be securely maintained. While testing the Department's security over its systems, auditors identified potential and actual vulnerabilities that existed within the Department's systems. Because of the nature of this finding, the specific details of the finding were verbally communicated to those officials directly responsible for implementing corrective action.

Effect: It is possible for unauthorized persons to obtain confidential data or make changes to computer programs or data. This finding is a significant deficiency in internal control over financial reporting.

Cause: The Department's existing network security controls were not properly configured.

Recommendation: The Department should take immediate action to correct the specific network security deficiencies identified and establish policies and procedures to prevent similar vulnerabilities.

Agency Response: Concur
Contact person: Cristy Schaan, Information Security Officer, (602) 716-6758
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: The Department took immediate short-term steps in mitigating the risk by removing the tool with vulnerabilities. The Department has designed a longer-term more comprehensive solution. Currently, we anticipate having the plan completed by September 30, 2010.

09-17
The Department of Economic Security's Division of Developmental Disabilities should strengthen computer access controls

Finding

Criteria: Access to computer systems should be limited to those employees authorized to process transactions or maintain a particular system and ensure that no one individual has the ability to modify data without an independent review.

Condition and context: The Division of Developmental Disabilities did not always adequately limit logical access to its claims payment system for Institutional and Home and Community-Based medical expenditures during fiscal year 2009. Specifically, 14 of the 39 users tested with administrative access had incompatible responsibilities or capabilities, including the ability to modify service rates, third-party liability waiver information, and payment addresses. In addition, 2 of 32 system users tested had incompatible responsibilities or capabilities that weren't necessary to fulfill their job responsibilities. Further, auditors noted an account having approval and update privileges that was not assigned to a specific employee.

Effect: Users may have access to unauthorized information and the ability to perform unauthorized functions. Excessive access rights may allow users to perpetrate and conceal errors and irregularities in the normal course of duties, resulting in fraud and the possible misstatement of financial information. This finding is a significant deficiency in internal control over financial reporting.

Cause: The Division did not follow its policies and procedures to ensure security over its claims payment system for Institutional and Home and Community-Based medical expenditures.

Recommendation: The Division should monitor and enforce the following policies and procedures that strengthen security over its claims payment system for Institutional and Home and Community-Based medical expenditures.

- Retain access request forms with the Supervisor's approval.
- Eliminate all generic user accounts and assign each user account to an individual employee.
- Limit access rights to those compatible with each employee's job responsibilities.

This finding was similar to a prior-year finding.

Agency Response: Concur

Contact person: Debra H. Peterson, Business Operations Administrator, (602) 542-6893
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: The Department will implement the audit recommendation. Specifically, the following actions have been taken to:

- Retain access request forms with the supervisor's approval.
  - Access for the FOCUS system (for Institutional and Home and Community-Based medical expenditures) is granted only through the J-125 process, which includes retention (hard copy or electronic) of the supervisory approval document. On September 17, 2009, internal retention of the access request forms was changed to follow the process flow of the request. This internal change strengthens security over the FOCUS claims payment system and enforces policies and procedures.
- Eliminate all generic user accounts and assign each user account to an individual employee.

  - Use of all FOCUS generic user accounts was eliminated, effective April 24, 2008, with the exception of one generic user account. This last generic user account was disabled on the FOCUS system November 11, 2009.
- Limit logical access to as few employees as possible and ensure access is compatible with each employee's job responsibilities.
  - The Division implemented policies and procedures in January 2008 to ensure that only authorized users have logical access. Such logical access is limited to essential employees, and that access is compatible with each employee's job responsibilities. The Division will implement a new process that will review user access by job description during the first quarter of each fiscal year. DDD completed the first review using the new process on December 15, 2009. In the future, DDD will complete these reviews by July 31 of each year.

09-18
The Department of Economic Security's Division of Developmental Disabilities should maintain required case file documentation

Finding
Criteria: Case management is the process in which services are identified, planned, obtained, and monitored for individuals eligible for Arizona Long Term Care System (ALTCS) services. The ALTCS Contract and *AHCCCS Medical Policy Manual* for case management require periodic on-site reviews within every 90 days or 180 days based on the applicable ALTCS member placement and service provided. The *AHCCCS Medical Policy Manual* requires that all contact attempted and made with, or regarding an ALTCS member be documented in the member's case file.

Condition and context: The Division of Developmental Disabilities did not ensure the required information was included in the member case files and that reviews occurred within specific time frames. Specifically, auditors noted that for 8 of 15 cases tested, reviews were not performed or were performed later than the required 90 or 180 days, and documentation for all contact attempts were not included in the case file.

Effect: This deficiency resulted in material noncompliance with the ALTCS Contract case management requirements.

Cause: The Division did not always follow its policies and procedures for case management.

Recommendation: The Division should monitor and enforce the following policies and procedures over case management.
- Perform the required on-site reviews within the required time frames.
- Document all contact attempted and made with, or regarding an ALTCS member.

Agency Response: Concur
Contact person: Debra H. Peterson, Business Operations Administrator, (602) 542-6893
Anticipated completion date: April 2010

Agency Corrective Action Plan: The Division will monitor retention of case file documentation to ensure that policies and procedures are followed.

The Division audits for timeliness of Support Coordinator visits in both its case file audit process and in a separate, focused timeliness audit (100% of the caseload for 10% of the Support Coordinators in each District). The results of these audits are compiled and analyzed at both the District and Statewide level. Corrective action plans are developed as needed. In addition, one component of the FOCUS application, alerts the Support

Coordinator when member visits are due and overdue. This automated process allows supervisors to monitor when timeliness issues are present.

In order to implement FY 2009 budget reductions for Senate Bill 1001, DES initiated staff reductions and furloughs that created higher caseloads and adjustments in workload. The Department continues to monitor caseloads, timeliness and requires corrective action plans at the individual and district level as needed. The Department continues to identify critical support coordination positions to fill and hires promptly when approved

09-19
Arizona State University should strengthen controls over payroll expenses

Finding
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.

This finding was similar to a prior year finding.

Agency Response: Concur
Contact person: Joanne Wamsley, Senior Associate Vice President and Deputy Treasurer, (480) 965-6940
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: In regard to the recommendations of the auditors in finding 09-19, Arizona State University's (ASU) 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 FY 2010. The University has enhanced existing policies and is 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) that 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 have 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 FY 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 FY 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 performed timely 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 rollout to all departments in FY 2010.

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

09-20
Arizona State University should strengthen controls over access and change management, and update its disaster recovery plan for its computer information systems

Finding
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.

This finding was similar to a prior year finding.

Agency Response: Concur
Contact person: Tina Thorstenson, Assistant Vice President and Information Security Officer, (480) 290-1551
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: 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 different 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 the Arizona Department of Administration (ADOA) and has business continuity procedures for the purpose of disaster recovery. ASU's hosting partner, 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 requirements 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 FY 2008. This process only ran periodically in FY 2009. Beginning the first quarter of FY 2010, this process is run daily. In the second half of FY 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.

09-21
Arizona State University needs to perform regular security risk assessments for its Web-based applications used to grant access to its computer systems

Finding
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.

This finding was similar to a prior year finding.

Agency Response: Concur
Contact person: Tina Thorstenson, Assistant Vice President and Information Security Officer, (480) 290-1551
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan:

- 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.

09-22
Northern Arizona University should strengthen access controls over its Web-based application

Finding
Criteria: The University should have effective access controls to prevent and detect unauthorized use, damage, loss, or modification of programs and data, and misuse of sensitive or confidential information.

Condition and context: The University uses a Web-based application to initiate, record, process, and report personnel information, payroll expenses, and student information. While testing the University's security over this application, auditors identified a number of potential and actual vulnerabilities that existed. Because of the nature of this finding, the specific details of the finding were provided to the University's president in a separate letter.

Effect: It is possible for unauthorized persons to obtain and misuse or modify confidential data. This finding is a material weakness in internal control over financial reporting.

Cause: The University was not aware of the vulnerabilities identified.

Recommendation: The University should take immediate action to correct the specific security deficiencies identified and establish policies and procedures to prevent similar vulnerabilities.

Agency Response: Concur
Contact person: Harper Johnson, Director of Information Security, (928) 523-7225
Anticipated completion date: March 2010

Agency Corrective Action Plan: The Information Security team in coordination with the ITS system administrators took immediate steps to correct the identified weaknesses and to implement improved controls.

09-23
Northern Arizona University should strengthen computer access controls

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

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

- The University did not have controls in place to ensure only authorized users had access to sensitive student, financial, and personnel data on its human resources, payroll, and student information system. Specifically, while performing test work on this system, auditors noted that a system password, which allowed access to sensitive data, was stored in an insecure manner.
- The University's database administration team, which consists of five people, uses a shared system administrative user name and password with unlimited privileges, which allowed them the ability to access and change data in the database. The database is the data warehouse for the University's main systems. In addition, the University did not review system activity logs for unauthorized activity.
- The University used a Central Authentication System (CAS) for authenticating system users. The system was supposed to lock out a user after six invalid logon attempts; however, auditors were able to enter incorrect passwords more than six times and were not locked out of the system. In addition, the University has no policies and procedures in place to lock out invalid logon attempts on systems that do not use the CAS for authentication.

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

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

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

- Limit the use of stored passwords and ensure strong encryption methods are used for any passwords being stored.
- Prohibit database usernames and passwords from being shared among system users.

- Maintain and review system activity logs and investigate unusual activity.
- Ensure the account lock-out policy is implemented and utilized on all systems.

Agency Response: Concur
Contact person: Harper Johnson, Director of Information Security, (928) 523-7225
Anticipated completion date: May 2010

Agency Corrective Action Plan:

- Recommendation 09-23a – Limit the use of stored passwords and ensure strong encryption methods are used for any passwords being stored.

  Response 09-23a – A review of stored password usage has been started to ensure that any remaining stored passwords follow the standards requested. The review will be completed by February 2010.

- Recommendation 09-23b – Prohibit database usernames and passwords from being shared among system users.

  Response 09-23b – The database administration team will implement controls to allow for auditing of changes made by individual administrators. This process will be completed by May 2010.

- Recommendation 09-23c – Maintain and review system activity logs and investigate unusual activity.

  Response to 09-23c – The Information Security team in coordination with the ITS system administrators will purchase and implement log monitoring software that will better alert administrators to log anomalies requiring investigation. Completion Date is March 2010.

- Recommendation 09-23d – Ensure the account lock-out policy is implemented and utilized on all systems.

  Response 09-23d – The University's account lock-out rules will be enforced by changes to the Central Authentication System (CAS) by March 2010. A password management policy will be created and implemented for non-CAS systems by May 2010.

09-24
Northern Arizona University should strengthen computer change controls

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

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

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

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

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

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

This finding was similar to a prior-year finding.

Agency Response: Concur
Contact persons: Patrick Benson, Director of Administrative Computing, (928) 523-8221 and Harper Johnson, Director of Information Security, (928) 523-7225
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan:
This is a complex finding and several efforts are underway to address the recommendations.

- Recommendation 09-24a – Log, authorize, test, review, and approve all program changes to computerized systems prior to implementation. In the event of an emergency, ensure the nature of the emergency and that the change made is subsequently documented, reviewed, and approved.

  Response 09-24a – The Oracle/PeopleSoft application suites have required Service Order System (SOS) tickets since 2007. As noted below in the response to Recommendation 2, shortcomings with the current SOS system noted above may have resulted in loss of full information about some changes. This will be addressed with release of the new SOS in June 2010. Policy, vendor supplied and locally extended technology support a robust production environment change management process for Oracle/PeopleSoft application suites. The Configuration Management Team (CMT), an ITS unit under Computing and Communication Services and independent of the Administrative Computing development teams, controls change implementation.

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

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

- Recommendation 09-24b – Monitor all system change requests with a log or report-tracking system to ensure that all requests have been authorized, assigned resources, tested, reviewed, and approved.

Response 09-24b – There is an in-place system to monitor and track change requests, the ITS Service Order System, SOS. The in-place system has shortcomings. Currently, SOS allows an accidental or intentional overlay of information and history. This could result in incomplete or misleading information about a change being retained. This shortcoming is being addressed as a work item in the in-progress rewrite of that system. Specifically, no user will be able to change or delete technical and functional comments after entry. The issue of SOS changes resulting in information overlay identified is being addressed by technology that retains information (including comments, status, etc) uniquely so subsequent or multiple work items do not obfuscate or destroy other or earlier information.
CITO Fred Estrella has set a June 1, 2010, for the replacement system to be in-place and fully functional.

- Recommendation 09-24c – Retain documentation to support that program changes were authorized, tested, reviewed, and approved.

  See the response to Recommendation 09-24b.

09-25
Northern Arizona University should test its disaster recovery plan

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

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

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

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

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

Agency Response: Concur
Contact person: Harper Johnson, Director of Information Security, (928) 523-7225
Anticipated completion date: March 2010

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

The other auditors who audited the Department of Transportation reported the following material weakness.
09-26
Department of Transportation
Liabilities not accrued

Finding
Criteria: The design and operation of the components of internal control over financial reporting should reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material to the financial statements may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Condition: Certain liabilities relating to the reporting year were not accrued. Management has a process wherein expenditures incurred for contract work during the fiscal year that are not paid until after year-end are reviewed to determine recognition in the correct period based upon the date the work is performed as described in the supporting documentation. However, this review was not performed properly for certain contract expenditures during the absence of employees responsible for coding the correct period. This resulted in a material amount of liabilities not being accrued as of June 30, 2009. Management recorded an adjusting entry to correct the error.

Context: This finding was identified as a result of audit tests, including sampling disbursements made subsequent to June 30, 2009, and determining whether those disbursements related to the year ended June 30, 2009.

Effect: Other accrued liabilities and expenditures in a nonmajor governmental fund were inadvertently understated by $6.8 million. This resulted in management recording adjusting entries to correct this error in the June 30, 2009, financial statements.

Cause: Management did not have procedures in place to review the cutoff of contract expenditures in the absence of personnel trained in this area.

Recommendation: We recommend that management strengthen its policies and procedures over identifying and recording contract expenditures in the correct period.

This finding was similar to a prior-year finding.

Views of Responsible Officials and Planned Corrective Actions: As of September 2009, the contracts payable unit now reports to the accounts payable manager. Several changes have already been implemented and new year-end procedures will be in place, and the staff trained, regarding those procedures before fiscal year-end 2010. The accounts payable manager will also verify and approve the documents input into the system after June 30 to ensure proper coding.