08-01
The Department of Administration should seek the authority to enforce rules over financial reporting

Finding

The Director of the Department of Administration 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 do not include provisions to enforce compliance.

Consequently, the Department did not always receive timely financial information from the agencies and was not able to issue the State’s fiscal year 2008 CAFR by its scheduled December 31, 2008, deadline since state agencies did not comply with the established deadlines. For example, 17 state agencies had a December 1, 2008, deadline to submit their audited fiscal year 2008 financial statements. Only seven agencies met this deadline, and some did not submit their audited financial statements until several months later, one as late as March 9, 2009. As a result, the State did not issue its CAFR until May 2009.

Such delays in financial reporting may result in the State’s ratings for bonds and certificates of participation being lowered by the rating agencies. Also, the State’s Single Audit Reporting Package will be issued late, which could result in a loss of federal funding.

This finding is considered a material weakness over financial reporting.

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

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

A similar recommendation was provided to the Department in the prior year.

Agency Response: Concur

Contact person: Clark Partridge, State Comptroller, (602) 542-5405
Anticipated completion date: June 2010

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 will explore potential options for enforcement actions and continue to work with state agencies to effectively resolve the issue of timely submission of financial information.

08-02
The Department of Administration should establish fraud prevention and detection programs

Finding

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. To help accomplish these objectives, the Department should establish a statewide antifraud program or other methods to promote ethical behavior. Individual state agencies may have controls designed to mitigate specific risks of fraud. However, the Department has not established a statewide program that addresses fraud risk due to inadequate resources.

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:

1. A state-wide program designed to prevent, deter, and detect fraud and promote a culture of honesty and ethical behavior.

2. A communication channel for citizens and employees to report suspected unethical behavior, fraud, or code of conduct violations.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Concur
Contact person: Clark Partridge, State Comptroller, (602) 542-5405
Anticipated completion date: Completed

Agency Corrective Action Plan: 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:

1. Assigning responsibility for reporting fraud, theft, waste or abuse;

2. Providing guidelines to conduct investigations of suspected fraudulent behavior; and

3. Requiring each employee to attend bi-annual fraud awareness training.

08-03
The Department of Administration’s Benefits Office should strengthen controls over claims payment processing for the State’s self-insured health benefits program

Beginning in fiscal year 2005, the State implemented a self-insured health benefits program for its employees and retirees, and their dependents. The Department of Administration’s Benefits Office is responsible for administering this program. For healthcare claim payments, the Benefits Office contracted with seven vendors to process and pay all medical and prescription drug claims for the program. These vendors processed approximately $682 million in medical and prescription drug claims during the fiscal year. Therefore, it is critical that the Benefits Office require these vendors to have an effective system of internal control in place to ensure that claim payments are accurate and appropriate. However, the Benefits Office did not fully accomplish this objective. Specifically, one vendor that was responsible for applying contractual discounts to medical claims (i.e., repricing) that processed approximately $17.3 million in claims during the fiscal year, did not receive an independent audit to ensure that this was done in accordance with its state contract because the Benefits Office did not include the audit provision in the vendor’s contract. Further, the Benefits Office did not perform its own audit of the claims paid because this vendor did not provide the Benefits Office with its fee schedules used for payments to medical providers.

To strengthen controls over the medical and prescription drug claims payment process, the Benefits Office should establish and follow the policies and procedures listed below:

1. Establish contractual provisions requiring vendors that reprice medical claims to have an effective internal control system to accurately and appropriately reprice medical claims in accordance with the contracts.

2. Obtain an independent annual audit of the vendor’s repricing processing controls to determine whether controls have been placed in operation and are operating effectively or conduct its own audit of claims-payment data to ensure that claims are paid for allowable services to eligible plan members only, in accordance with vendor fee schedules and the proper application of copayments.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Concur
Contact person: Philip Hamilton, Assistant Director Benefit Services Division, (602) 542-4501
Anticipated completion date: October 2009

Agency Corrective Action Plan: Issues regarding repricing of claims were generally resolved with the mutually agreed upon termination of contract with Schaller Anderson effective September 30, 2008. Schaller Anderson was the only contractor in such an arrangement due to their proprietary fee schedule and their reluctance to submit said fee schedule to the Third Party Administrator (TPA).
To strengthen controls over the medical and prescription drug claims payment process, BSD (Benefit Services Division) has taken the following actions:

- Requests for Proposal (RFP) and the subsequent contracts for the plan year beginning October 1, 2009 require vendors that process medical and/or prescription

drug claims to have an effective internal control system and the vendor must conduct a type II SAS70 audit at least annually at no cost to the State.
 RFP and the subsequent contracts for the plan year beginning October 1, 2009 require vendors to provide unrestrictive operational and financial audit rights to ADOA or an ADOA approved independent auditor to conduct such audits at any time during the contract term. The vendor must not limit the time period of claims to be audited and the vendor must be responsible for payment of an auditor.

The vendors are also required to put fees at risk for performance guarantees regarding the accuracy and timeliness of claim processing.

08-04
The Department of Administration should strengthen controls over the Human Resource Information Solution (HRIS) account management

Account management, which includes the request, approval, establishment, suspension, and termination of user accounts, is an integral part of system security. Therefore, it is vital that the Department develop and implement policies and procedures for account management over its HRIS system. However, due to a lack of resources, the Department did not develop comprehensive policies and procedures over account management for operating system accounts, application administrator accounts, or database management system accounts. In addition, certain operating system and database management system accounts were shared among HRIS team members, the passwords for these accounts were not periodically changed, and current HRIS policies did not address how often passwords should be changed. Also, although activity logs did track user access and changes made to hours worked and salaries, these logs were not monitored regularly. Finally, there were no controls to prevent HRIS administrative users from changing these logs.

To strengthen controls over HRIS account management, the Department should strengthen existing HRIS policies and procedures by performing the following:

- Develop comprehensive policies and procedures for operating system accounts, application administrator accounts, and database management accounts.

- Require that HRIS administrators' user access is appropriately changed when they're assigned to different positions or responsibilities to help ensure that no individual has access to various types of administrator accounts.

- Prohibit sharing HRIS administrator user accounts, and require that users change passwords at least quarterly.

- Ensure that adequate controls are in place to prevent unauthorized changes to activity logs and that the logs are monitored on a regular basis.

A similar recommendation was provided to the Department in the prior year.

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

Agency Corrective Action Plan: Since this finding, HRIS has implemented sudo access to its administrator accounts (LAWSON, HRISMSTR). Passwords for administrative accounts get changed on a monthly basis by the system administrator and shared with the HRIS Manager. A script is being developed that will automatically change the administrator accounts passwords, eliminating the need for anyone to know those passwords since sudo is in place. The estimate on script implementation is May 2009.

We now have a Lawson system administrator. Prior, the database administrator (DBA) performed many of these responsibilities that required he have access to root. This is no longer the case and DBA are granted only the root level access necessary to perform their job duties.

Sharing of HRIS administrator user accounts/passwords no longer occurs due to the implementation of sudo access to these accounts. Password aging for all HRIS users (Power, MSS and Y.E.S.) will be rolled out in June 2009 as a result of the new security features of the LSF9 environment upgrade.

Database logs are used by DB2 to keep the database consistent if a restore was necessary from back-up due to a database crash. DB2 logs are transaction logs and should not be updated by anyone (DBA or otherwise). If a DB2 log were to be tampered with, the database would disassociate itself from the log(s) and return errors.

When HRIS upgrades to application version 9.0 (estimate 12/31/09), more auditing features will be introduced into the overall design of the application. User ID, date and time stamps have been added to numerous “control” tables in Lawson.

08-05
The Department of Administration should improve controls over HRIS system changes

Changes to computer programs must be monitored and tested to ensure that a computer system is functioning properly. However, due to a lack of resources, the Department did not develop adequate written policies and procedures for changes to its HRIS system, including procedures for operating system changes and the testing of application changes. In addition, adequate documentation of operating system changes was not always prepared and retained. Also, the system did not generate a log to help monitor operating system and table changes, and the log for application changes was not reviewed on a regular basis. Finally, controls were not in place to detect changes made directly to the system’s database.

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

- Develop adequate written policies and procedures for all types of program changes, including operating system changes and the testing of application changes. Further, these policies and procedures should include procedures for the design, testing, approval, documentation, and implementation of system changes.

- Document all system changes, including identifying number, program code modifications, test results, approvals, and implementation dates. This documentation would be a valuable resource when planning additional system changes or if a system failure occurred.

- Develop a system-generated change log to track all changes, and periodically review it to ensure that all changes were authorized, tested, and properly implemented.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Concur
Contact person: Jody Piper, HRIS Manager, (602) 542-4282
Anticipated completion date: Complete

Agency Corrective Action Plan: Written policies and procedures have been created.

All system changes are tracked through Project Office. Included as attachments are test results, approvals, and dates that changes were implemented into production. Also, all changes are verified and promoted using the Tripwire utility. The Tripwire report shows the date/time system changes were introduced into Production HRIS. Another spreadsheet lists all modifications to the Lawson application system. This spreadsheet is updated by the Quality Assurance Manager when new customizations are introduced into the HRIS system. The HRIS management team uses this document when analyzing upgrades and patches from the vendor to determine if the modifications are still needed. If it is determined the modifications are still needed, the spreadsheet allows management to determine the level of effort needed from the team to retro-fit code, test and deploy the customization.

Tripwire has been installed on the HRIS systems. This utility generates reports for operating system (OS) level, application and database level changes. The Tripwire report is reviewed daily by HRIS management and system administrators for OS, application and database changes to ensure all changes were authorized by either a CCF (Change Control Form) or Change Request from the Change Control Board. The Tripwire report is also reviewed by the HRIS security team to ensure that all OS User accounts created by the system administrators came from requests generated by the New User security procedures.

08-06
The Department of Administration’s State Procurement Office (SPO) should ensure the SPIRIT System Administrator and Procurement Systems Manager do not have access to data

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. SPIRIT’s Web interface replaces the previous paper-based procurement process. An adequate method should be maintained to monitor all changes to the system. Currently, the SPIRIT System

Administrator and Procurement Systems Manager have access to data on the SPIRIT system in order to revise vendor bids at the vendor's request. To document such changes, the Office maintained only a manual log. As a result, vendor bids could be changed with no written documentation from the vendors.

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 and Procurement Systems Manager from having the ability to change system data.

- Enable the logging function in the database to track administrator user changes through an automated log, journal, time stamp, or other applicable method that would document the change.

- Have the vendor resubmit the bid or simply add an amendment to the original document.

- Require vendors to submit signed, prenumbered forms that list the changes made and the reasons for them.

Agency Response: Concur
Contact person: Jean Clark, State Procurement Administrator, (602) 542-9136
Anticipated completion date: September 1, 2009

Agency Corrective Action Plan: The new eProcurement system will prevent SPO staff from accessing the data except through the use of the application, which has the appropriate tracking mechanism and security controls in place.

08-07
The Department of Administration's State Procurement Office needs to ensure more than one person is capable of maintaining the SPIRIT Web application

The Department of Administration's State Procurement Office should minimize overdependence on key individuals through documentation, knowledge sharing, succession planning and staff backup. The development, updating, and maintenance of the SPIRIT Web application is solely dependent on one person employed by a third-party contractor who possesses all of the critical knowledge necessary to effectively perform these functions. In the event that the individual leaves the contracted consulting organization, neither the contractor nor the SPO would have employees with the knowledge to effectively update and maintain the SPIRIT system.

To help ensure the continued maintenance of the SPIRIT system, the SPO should develop a contingency or replacement plan. This could entail requiring the contracted organization to employ other persons with the knowledge necessary to maintain the system, requiring the developer to maintain detailed documentation regarding the development and operation of the application so that others could take on that role, training in-house employees to maintain the SPIRIT system, or planning for replacement of the system using more current technology.

Agency Response: Concur
Contact person: Jean Clark, State Procurement Administrator, (602) 542-9136
Anticipated completion date: September 1, 2009

Agency Corrective Action Plan: The new eProcurement contractor has a current development staff of six and a support staff of six, which are capable of making configuration and customization modifications as well as troubleshooting the application.

08-08
The Department of Administration's Information Systems Division (ISD) should strengthen access controls over its SPIRIT system

System access controls help ensure that only authorized users have access to the SPIRIT system. These controls are critical in protecting sensitive information, and preventing and detecting unauthorized use, damage, loss, or modification of programs and equipment. System access controls restrict not only physical access to the system, but also logical access to the system. Logical access includes access granted to users who are responsible for processing transactions on the system, as well as access granted to database administrators who have unlimited access and are responsible for maintaining the system. The ISD has policies and procedures to control both types of access; however, administrative access control lists were not reviewed after changes were made to the system or on a regular basis. Further, the application developer has access to SPIRIT production design templates. As a result, the application developer or other users could modify a production design template file before database administrators use the template to update the design of a production database.

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 production design templates. Further, an ISD employee should review access control lists on a monthly basis.

Agency Response: Concur
Contact person: Jean Clark, State Procurement Administrator, (602) 542-9136
Anticipated completion date: September 1, 2009

Agency Corrective Action Plan: Having access to the production template does not allow access to the production data; however, the DRM SPIRIT application migration procedures have been modified to add a new step to remove the developer's access to the production template after a SPIRIT application migration has occurred. The current SPIRIT production database templates have been modified as well to reduce the developer's access level to "reader". The revised SPIRIT Application Migration Checklist includes the additional step.

ACL modification is restricted to two DRM staff members. All modifications made to an ACL have generated and will continue to generate an e-mail to the primary SPIRIT DBA, which notifies her of the change and the e-mail messages are archived within GroupWise. We have added a new activity to perform a monthly review of production ACLs, which will be performed by the DBA and will occur during the first week of every month.

08-09
The State should verify that servicing banks have effective internal controls

Various state agencies have contracted with commercial banks to process the State's cash receipts. This includes using a servicing bank to collect and process taxes, fees, fines, and various other state agency cash receipts, as well as maintaining operating accounts used to deposit tuition and fees, federal monies, and other receipts. These receipts are in the form of cash payments, wire transfers, and credit card receipts. Therefore, as these banks collect, process, and transmit confidential and sensitive financial information, it is imperative that they have effective systems of internal controls for processing, recording, and reporting these receipts to the various state agencies. However, the State did not have procedures in place to monitor internal controls at the servicing banks to ensure that the banks' controls were operating effectively. Further, the contracts with the servicing banks did not always require the banks to obtain an assurance review performed by an independent third party to help ensure controls at the banks are sufficient to protect the integrity of the State's financial information. As a result, assurance reviews were not performed annually for all of the State's servicing banks.

To help ensure services provided by the State's servicing banks are in accordance with contract provisions and that the servicing banks have an effective system of internal control for processing financial transactions of the State and its agencies, the State should establish and follow the policies and procedures listed below:

- Ensure that servicing bank contracts include all services to be provided.

- Verify that the servicing banks have effective internal control systems to accurately process and record the State's financial transactions and safeguard confidential and sensitive financial information. To help determine whether controls have been placed in operation and are operating effectively, the State should establish contractual provisions requiring the State's servicing banks to have their internal control systems that process and record the State's financial transactions audited annually. In addition, assign a state agency to review these audit reports and require a corrective action plan if deficiencies are noted.

- Monitor all other contractual provisions for compliance.

- Ensure that state agencies have effective controls in place to validate the accuracy of transactions processed by the servicing banks.

A similar recommendation was provided to the State in the prior year.

Agency Response: Concur
Contact person: Clark Partridge, State Comptroller, (602) 542-5405
Anticipated completion date: July 2012

Agency Corrective Action Plan: The State understands the importance of internal controls on processing cash receipts and related data, and has established controls to address the related risk. We will continue to coordinate our activities to ensure that state information is processed in an appropriate environment.

08-10
The Industrial Commission of Arizona needs to strengthen controls over financial reporting

The State of Arizona 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. 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) has established timelines for the individual state agencies to submit required financial information to it for inclusion in the state-wide financial statements. The Commission's management is 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 January 14, 2009, approximately 3 months late, and its final financial information on March 27, 2009, approximately 5 months late. The delays resulted from the Commission 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. Further, the Commission is dependent on a single employee who possesses all of the critical knowledge necessary to effectively make all adjusting entries and compile the financial statements. In the event that the employee leaves the Commission or is unable to perform his responsibilities, other employees would not possess the knowledge to accurately or efficiently compile the financial statements.

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.

A similar recommendation was provided to the Commission in the prior year.

Agency Response: Concur
Contact person: Gary Norem, Chief Financial Officer, (602) 542-4653
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

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. There currently are no plans to make changes to the general ledger system until at least 2015.

The staffing situation was improved by establishing a new higher level accounting position in March of 2008 to specifically handle the Special Fund general ledger and financial statement preparation work. A permanent staff member was hired May 5, 2008, which should improve the situation in future years. In addition, more cross-training of other accounting staff members during the 2010 fiscal year will develop back-up staff that can fill in when a staffing emergency occurs.

The Chief Financial Officer (CFO) has 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 2009 will be completed by October 15, 2009 and the final statements completed by November 5, 2009.

08-11
The Industrial Commission of Arizona should develop written policies and procedures for its computer operations

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. Reliance on appropriate written policies and procedures can enhance both accountability and consistency, and safeguard assets and data. However, the Commission had not established detailed written policies and procedures over its computer operations due to a lack of resources.

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 PACE 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 control—There should be procedures that address the request, approval, establishment, suspension, and termination of user accounts since this is necessary for system security.

A similar recommendation was provided to the Commission in the prior year.

Agency Response: Concur
Contact person: Gary Norem, Chief Financial Officer, (602) 542-4653
Anticipated completion date: Complete

Agency Corrective Action Plan:

- Daily operations and physical security procedures for the PACE programs have been created and are in use.

- Procedures regarding adding, editing, suspending, and terminating user accounts as related to all operating system platforms and agency IT programs, including the PACE system, are in place.

08-12
The Industrial Commission of Arizona should maintain a record of all changes to its computer system

The Commission uses the PACE computer system to record detailed financial transactions and generate monthly and year-end summary reports to support amounts recorded on the general ledger. Therefore, it is essential that changes to the system and data be documented; however, this wasn't always done due to a lack of resources. 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. As a result, unauthorized changes could be made to the system or data without detection.

The Commission should maintain a record of all system changes on the PACE system to help monitor changes and ensure they have been properly authorized.

A similar recommendation was provided to the Commission in the prior year.

Agency Response: Concur
Contact person: Gary Norem, Chief Financial Officer, (602) 542-4653
Anticipated completion date: Complete

Agency Corrective Action Plan:
In fiscal year 2009, the ICA implemented a program change form in the event a PACE program change is required. However, based on the fact that PACE is an unsupported Legacy application and the previous developer/administrator retired in 2008, it is not anticipated any program changes will be attempted in the future.

As a result, the ICA is currently developing software to replace the PACE system.

08-13
The Department of Revenue’s computer access controls should continue to be strengthened

Access controls restrict physical and logical access to the Department’s computer systems. These controls help ensure that only authorized users have access to the Department’s computer systems and are critical in protecting computer systems and data from unauthorized use, damage, loss, modification, or disclosure. While the Department has established policies and procedures to control computer access, it did not always follow its policies and procedures to adequately protect its systems and data. Specifically, the Department did not maintain audit logs to periodically monitor the activities of its database administrators and other individuals with elevated system access. These individuals had unlimited access to data stored on the Department’s tax system. In addition, system access rights were not always appropriately modified or terminated when a department employee, agent, or contractor was either transferred to another position or was no longer working for the Department, nor were system access rights always appropriate for users’ assigned job responsibilities. Further, physical access to the Department’s computer room was not restricted to only essential employees. Finally, the Department had policies to ensure that its temporary employees, agents, and contractors were aware of federal and state guidelines governing confidentiality of taxpayer information; however, procedures were not implemented to enforce these policies.

The Department should strengthen its policies and procedures over access to its computer systems and data to help prevent or detect unauthorized use, damage, loss, modification, or disclosure. Only authorized users should have logical or physical access to the Department’s computer systems, and access should be limited to essential employees only. While the Department currently has certain controls in place over logical and physical access, it should continue its efforts to strengthen controls by:

- Periodically monitoring the activities of database administrators and other individuals with elevated system access.

- Maintaining proper system access rights for each department employee, agent, and contractor. This includes modifying or terminating system access rights immediately after an individual is either transferred to another position or no longer working for the Department, retaining access change authorizations, and ensuring access rights are appropriate for each individual’s job duties and responsibilities.

- Restricting physical access to the computer room to only those employees who need access to perform their job duties and responsibilities. Further, the Department should conduct periodic reviews of those who have access and remove or modify access rights as necessary.

- Training temporary employees, agents, and contractors on the federal and state guidelines governing confidentiality of taxpayer information on an annual basis in accordance with department policy.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Partially 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 takes the Auditor General's findings and the correction of those findings very seriously. As such, the Department has significant concerns with the Auditor General's statement," . . . a similar recommendation was provided to the Department in the prior year." This statement could leave the reader with the inaccurate perception that the Department has taken no action to address the Auditor General's findings. Further, because the findings are so broad in nature and because an acceptable margin of error has not been defined, the Department is concerned that there is no way to ever fully satisfy the finding.

Database Administrator Monitoring
As stated in its response to the Auditor General's 2007 Single Audit, the Department acquired the ability to log its database administrator activity. Since August 2008 Information Security (IS) has continuously captured database administrator activity to help ensure the integrity of the information and delivers the logs to a secured server accessible only by IS personnel. Subsequently, the Department purchased a Security Event and Incident Management tool named TriGeo, which will better facilitate the analysis and monitoring of those logs and, therefore, database administrator activities. The Department anticipates having the TriGeo tool in operation by the end of fiscal year 2009.

User Access Controls
As stated in the response to the Auditor General's 2007 Single Audit report, in February 2008 IS began reviewing the Vacancy Tracking Report (VTR) on a weekly basis to acquire necessary employee hire, transfer, and termination notifications in order to update user access controls. To further solidify the process, the Department will be shifting the oversight and coordination responsibility for this process to the Human Resources Unit, with secondary responsibility for the actual modification of access rights residing with the IS Unit. The Department anticipates with the reorganization of this process that user access modifications will be completed in no longer than two weeks.

Regarding access to vendors and contract staff, in fiscal year 2008 the Department began placing an expiration date on network accounts that will disable their accounts three months from the date of activation. To reactivate the account, the manager must submit a request to IS to extend the expiration date. In addition, IS monitors network accounts and disables accounts for which there has been no log-in activity for 60 days. If IS has not received within the next 60 days a request/justification to activate the account, the network account and all corresponding system accounts, e.g., BRITS, are deleted.

Furthermore, the Department will continue to improve the access control process by performing a complete one-time recertification of all IS managed systems access beginning in fiscal year 2010.

Physical Access

The Department has been continuously working to improve access to the second floor computer rooms. Managing access to the rooms is complicated by the fact that the Department does not completely own this process; the Department of Administration (DOA) owns the room and owns the badging system and management of that system. To better facilitate improvements for access management, the Department will more clearly document all personnel with approved room access and will document Department personnel that can approve access to those rooms. The Department will provide this documentation to DOA and IS will continue a bi-monthly review of DOA badge access reports.

Confidentiality Agreement

In order to obtain federal tax information from the Internal Revenue Service, the Department must have a confidentiality awareness program. The Department's awareness program requires each vendor with access to confidential information to sign a certificate to confirm receipt of information concerning federal and state confidentiality requirements.

To ensure that the certificates are always completed, all department sections utilizing vendor services will be required to complete a vendor worksheet identifying the vendor's name and location, work to be performed, time period of provided services, as well as a list of the vendor's employees or subcontractors who will also have physical and/or computer access to confidential taxpayer information. A copy of this form will be sent to the Department's Disclosure Officer, who will use it to verify that the appropriate confidentiality certification is obtained.

Auditors' Comment to the Department of Revenue's Corrective Action

The Department of Revenue's officials responded that they partially concurred with findings 08-13 and 08-16 because they had concerns regarding the statement that some recommendations were previously provided in the prior year. The Department's responses point out efforts made to take corrective action as a result of the audit for the year ended June 30, 2007; however, the corrective action was implemented either late during fiscal year 2008 or after year-end. Therefore, the auditors' reference to similar findings in prior audits is factual and part of the standard reporting process.

The Department's responses provide the opportunity to explain its efforts, whether planned or implemented, to correct the findings, and agency responses have not been audited. The acceptable margin of error that auditors use when evaluating whether the State's financial statements are fairly stated, in all material respects, may not be consistent with operational effectiveness expected by a department's leadership or stakeholders. As a result, it would not be appropriate for the auditors to dictate such benchmarks. While the findings were characterized as "broad" by the Department, the auditors have communicated our concerns in greater detail throughout the audit to the appropriate personnel and they have acknowledged an understanding of the deficiencies. The Department's responses also include detailed actions taken to address the deficiencies, which further makes the Department's position unclear that the deficiencies are too broad in nature to correct.

08-14
The Department of Revenue should continue to improve controls over computer system changes

To help ensure that a computer system functions properly and provides safeguards over confidential and sensitive information, it is essential that changes made to the system are properly authorized, developed, tested, reviewed, and approved. It is also important to have testing, rollback, and communication plans for all significant system changes. These plans are intended to ensure changes have the expected effect on the system, allow the Department to reverse any changes that may adversely affect the system, and advise the appropriate personnel of pending changes and their potential impact. However, the Department did not ensure that program changes to its Business Reengineering Integrated Tax System (BRITS) were properly authorized, tested, reviewed, and approved by system users prior to implementation. For example, the Department did not always document the approval of program changes by the appropriate division managers or users. Additionally, it did not document testing, rollback, and user communication plans for significant changes to its tax system. Further, the Department needs to limit the number of individuals who have authority to move program changes into production. Specifically, there were 55 department employees and contractors who were authorized to move program changes into production. Many of these individuals had additional privileges and conflicting responsibilities, making it difficult for the Department to adequately monitor and review the activities of this critical function. Finally, there were insufficient controls for changes to other systems.

While the Department currently has certain controls in place over computer system changes, it should continue to improve controls to help:

- Ensure that users and management authorize, test, review, and approve all program changes to department systems prior to implementation and ensure documentation of all program changes is retained.

- Ensure testing, rollback, and communication plans for all significant program changes are developed and followed.

- Restrict the authorization for executing changes into production systems to only essential individuals. Also, ensure all program changes are reviewed, approved, and tested by an independent person.

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 Department recognizes the need for vigorous controls over computer program (production system) changes and has made major improvements towards this goal. In previous years the Business Reengineering/Integrated Tax System (BRITS) system changes were tracked exclusively in the BRITS Program Change Portal and Information Technology (IT) used a manual process to track other non-BRITS changes, such as software patches, updates, new server additions or network changes.

As part of an on-going improvement initiative, in mid-fiscal year 2008 and continuing into fiscal year 2009, IT developed a more robust formal change management policy, standards, procedures and utilizes a new tracking tool; IT no longer utilizes the BRITS Portal as a change management tool. Although IT keeps configuration management records in the Portal, the approval, testing plan, rollback plan and communications are stored in IT's Change Management Request (CMR) system. This new tool helps ensure appropriate risk ratings based on system criticality and also provides control by appropriate approval and division of duties of IT employees.

In addition, a Change Advisory Board (CAB) has been created comprised of the Chief Information Officer and all IT administrators, with additional business users to be added in early fiscal year 2010. Per the revised Change Management Policy, anyone requesting a system change must complete an online Change Request form, which is submitted to the Board for approval. The Board evaluates any risks associated with the change before granting its approval. Further, policy dictates that "any change that has the potential to impact the production environments must be recorded, reported to the CAB, scheduled and approved by the appropriate Change Manager" before the change can be put into the production environment. The CAB also reviews the implementation for success and, if necessary, provides rollback of the change.

08-15
The Department of Revenue should accurately report taxes receivable balances

The Department of Revenue is responsible for accurately accounting for and reporting its taxes receivable balances in the State's financial statements. While the Department has made substantial improvements for reporting these balances, the year-end taxes receivable balances the Department reported for inclusion in the State's financial statements were overstated by more than $2.7 million. Specifically, the Department incorrectly calculated an adjustment to the amount accrued for sales tax receivables, resulting in a $4.7 million overstatement. In addition, the Department miscalculated a second adjustment to correct an inaccurately recorded taxes receivable balance, which resulted in a $2 million understatement. The State's financial statements were adjusted for all significant errors.

To help ensure that taxes receivable balances at June 30 are properly reported, the Department should develop and implement controls to ensure that adjustments to the taxes receivable balances are reviewed for accuracy by an independent employee.

Agency Response: Concur
Contact person: Tom MacConnel, Comptroller, (602) 716-6593
Anticipated completion date: July 2009

Agency Corrective Action Plan: As stated in its response to the Auditor General's 2007 Single Audit, the Department has faced many challenges transitioning to the new tax administration system, BRITS. When the conversion was completed and the Accounts Receivable Summary Report became available in June 2007, the Department made great strides to improve its procedures to help ensure that accounts receivable information is accurately recorded and reported.

In fiscal year 2008, the Department deposited over $14 billion in tax revenues and as of June 30 2008, gross accounts receivable consisted of 1.2 million transactions totaling over $392 million. To ensure accuracy, Revenue Accounting conducts regular reviews of transactions that could significantly impact accounts receivable balances. Staff determines any manual adjustments needed to ensure that the accounts receivable balances are accurate and in accordance with the State's accounting policies. While an independent review of adjustments is a standard practice in the Department, unfortunately a review did not take place in this instance.

08-16
The Department of Revenue needs to continue improving data security management and security awareness

The Department of Revenue maintains confidential and sensitive taxpayer data that, if not adequately protected, could potentially be subject to loss or improper disclosure. The Department provides training to its employees, agents, and contractors on its policies for handling confidential taxpayer information and the penalties associated with the improper disclosure of such information. However, it lacked a comprehensive security program for the overall management of data security, including training for its employees, agents, and contractors on operating procedures for data security and increased security awareness. As a result of this weakness, auditors noted several instances in which confidential and sensitive taxpayer information was not adequately protected. Because of the sensitive nature of this finding, no further details will be reported here; however, this information has been communicated to the Department's director in a confidential letter. In August 2008, the Department began developing and implementing procedures to help mitigate the risk of loss or improper disclosure of confidential and sensitive information.

To help ensure confidential and sensitive taxpayer data is adequately protected from potential loss or improper disclosure, the Department should establish an entity-wide comprehensive security program addressing the overall management and education of data security and security awareness. This program should address all aspects of security and include a framework that provides for a continuous cycle of assessing risk, developing and implementing effective security controls, and monitoring the effectiveness of those controls. In addition, the program should provide on-going education of security awareness and practices to the Department's employees, agents, and contractors. Further, the Department's current security environment and access controls should be strengthened to help achieve effective data security management.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Partially 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 takes the Auditor General's findings and the correction of those findings very seriously. As such, the Department has significant concerns with the Auditor General's statement," . . . a similar recommendation was provided to the Department in the prior year." This statement could leave the reader with the inaccurate perception that the Department has taken no action to address the Auditor General's findings. Further, because the findings are so broad in nature and because an acceptable margin of error has not been defined, the Department is concerned that there is no way to ever fully satisfy the finding.

As stated in its response to the Auditor General's 2007 Single Audit, the Department continually strives to improve information security and has made vast improvements to its control environment. In October 2004 the Department initiated an Information Security (IS) program that reported within the Information Technology (IT) Division. As of 2006, that division now includes an IS Officer, an IS Engineer, an Analyst and two Specialists. The program was designed to manage four functional areas: 1) policy and compliance, 2) security events and incidents, 3) employee awareness and training and 4) access management.

Since its inception, IS has drafted a policy manual to provide standardized policy and compliance revisions to better organize security policies and operational and technical safeguards. In addition, standards and procedures have been established. For example, standards for network devices, servers and password management have been put in place and procedures for the review of security devices and servers and risk assessments and mitigations. The security program also includes an incident response program to capture, work, report and manage security incidents and events. Finally, should an incident be discovered, IS partners with the recently established Internal Audit unit (February 2007) and with Administrative Services to conduct internal investigations.

Furthermore, User Access Lifecycle Management has been centralized and access request and removal processes and documentation improvements have been made. Also, the process to map access for all user roles has begun.

In 2007 the Department formed an Information Security Steering Committee to provide oversight and recommendations over information security activities and concerns. The committee includes Department staff from various divisions that have governance roles related to the security and privacy of taxpayer data, information assets and physical security.

Information Security has worked with other governance staff to help establish an Employee Awareness and Training program. Information Security rewrote the Computer Use and Confidentiality Policy manual, tested user knowledge of Computer Use and Confidentiality Policy manual, created an agency newsletter "Security Spotlight" and plans to establish a new hire orientation security segment.

Despite staffing resources, IS continues to strengthen its current Employee Awareness and Training program, planning other education opportunities, such as working sessions and brown-bag type forums to disseminate security information and better educate the end user community about department security policies and procedures. The first training session planned for June 2009 will be directed towards IT staff and all staff taking training events will be documented.

Auditors' Comment to the Department of Revenue's Corrective Action
The Department of Revenue's officials responded that they partially concurred with findings 08-13 and 08-16 because they had concerns regarding the statement that some recommendations were previously provided in the prior year. The Department's

responses point out efforts made to take corrective action as a result of the audit for the year ended June 30, 2007; however, the corrective action was implemented either late during fiscal year 2008 or after year-end. Therefore, the auditors' reference to similar findings in prior audits is factual and part of the standard reporting process.

The Department's responses provide the opportunity to explain its efforts, whether planned or implemented, to correct the findings, and agency responses have not been audited. The acceptable margin of error that auditors use when evaluating whether the State's financial statements are fairly stated, in all material respects, may not be consistent with operational effectiveness expected by a department's leadership or stakeholders. As a result, it would not be appropriate for the auditors to dictate such benchmarks. While the findings were characterized as "broad" by the Department, the auditors have communicated our concerns in greater detail throughout the audit to the appropriate personnel and they have acknowledged an understanding of the deficiencies. The Department's responses also include detailed actions taken to address the deficiencies, which further makes the Department's position unclear that the deficiencies are too broad in nature to correct.

08-17
The Department of Revenue should reconcile income tax receipts to income tax revenues recorded on the Arizona Financial Information System (AFIS)

The Department's management and state officials depend on accurate financial information so they can fulfill their oversight responsibility, report accurate information to the public, and ensure that accurate information is reported in the State's financial statements. Reconciling tax receipts recorded on the Department's tax systems to the AFIS, the source of the State's financial statements, allows the Department to resolve any timing and other differences in a timely manner. Accordingly, starting in December 2007, the Department prepared monthly reconciliations of individual income tax revenues; however, the Department did not reconcile individual income tax revenues recorded on its legacy system for the first 5 months of the year. Auditors noted differences between the legacy system and the AFIS that the Department was unable to resolve.

To help ensure that accurate and complete information is recorded on the AFIS and reported in the State's financial statements, the Department should continue to reconcile all income tax revenues recorded on its systems to the amounts recorded on the AFIS at least monthly. In addition, the Department should promptly investigate all differences noted and make all necessary corrections.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Concur
Contact person: Tom MacConnel, Comptroller, (602) 716-6593
Anticipated completion date: January 2008

Agency Corrective Action Plan: As stated in its response to the Auditor General's 2007 Single Audit, the Department's legacy system did not have the necessary functionality to complete monthly reconciliations to compare the system's individual income tax revenue information against AFIS. Since the functionality became available on December 3, 2007 with the new BRITS individual income tax release, Revenue Accounting has been conducting monthly reconciliations.

08-18
The Department of Revenue needs to ensure the completeness of electronic data transfers

Individual income taxpayers have the option of filing their tax returns and payments electronically through a process known as e-file. Business taxpayers may submit returns and payments of sales taxes and income tax withholdings through the Department of Revenue's AZTaxes Web site. Corporate income taxpayers may also use the Department's Web site to remit payments. All electronic return and payment information is received, stored, and processed through a series of servers prior to being recorded on the Department's tax system. However, the Department did not have adequate procedures to ensure the completeness of electronic transactions transferred to the Department's tax system. Failure to reconcile the total number of electronic transactions recorded on the Department's system could result in missing transactions and inaccurate taxpayer accounts.

To help ensure that all electronic data transfers are complete, the Department should develop and implement policies and procedures to ensure that all transactions received and stored on a server are reconciled to the transactions recorded on the Department's tax system. The reconciliation should be reviewed and approved by a supervisor, and all differences should be investigated and resolved.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Concur
Contact person: Tom MacConnel, Comptroller, (602) 716-6593
Anticipated completion date: July 2009

Agency Corrective Action Plan: The Department of Revenue's www.AZTaxes.gov Web site provides taxpayers with the ability to electronically file their transaction privilege tax (TPT) and withholding returns. In addition, individual income tax returns are electronically filed with the state through tax practitioners, selftax software and other venues.

As stated in its response to the Auditor General's 2007 Single Audit, the Department planned to implement an automated reconciliation process to ensure that all electronically filed returns are extracted to its tax administration system (BRITS). Due to limited information technology resources, the automated process cannot be implemented until July 2009.

Until the automated process is complete, the Department has and continues to conduct a manual reconciliation process for individual income tax returns. Due to the labor intensive effort of reconciling TPT and withholding tax returns, and because the automated method should be available in July, the Department has delayed completing manual reconciliations for these two tax types. If the automated reconciliation software release is significantly delayed, a manual reconciliation process will be developed and employed. In any case, the Department will conduct the fiscal year 2009 and current monthly reconciliations systematically once the automated system becomes available.

08-19
The Department of Revenue should continue to establish effective controls over its contracted services

The Department of Revenue contracted with vendors to perform certain tax processing services. These contracted services included printing and mailing tax refund checks and allowing taxpayers to make transaction privilege tax and other tax payments electronically. Therefore, it is critical that the Department requires these vendors to have an effective system of internal controls in place to ensure that tax refund checks are properly issued and that taxes collected are recorded accurately and deposited. In addition, the Department used vendors to perform data entry services of taxpayer returns. Because tax returns contain confidential data, it is critical that this information is securely maintained at all times. While the Department reviewed the audit report for one of its two primary vendors, it did not ensure that the other vendor had an effective system of internal control. Further, the Department did not ensure that data entry vendors had the appropriate security measures in place to secure taxpayer information. During the year, a vendor oversight committee was established to oversee the monitoring efforts of the Department’s contracted services. However, the committee was not able to make significant progress to mitigate the associated risks.

To help ensure contracted services are adequately monitored and that confidential taxpayer information is protected, the Department should continue to:

- Verify that vendors have effective internal control systems by annually reviewing the audit reports of each vendor’s internal control system or by performing procedures to determine the sufficiency of vendor controls.

- Establish policies and procedures to document the receipt and review of the audit reports of its vendors, including an analysis of the opinion provided within the report and a request for a corrective action plan if deficiencies are noted. In addition, the Department should implement internal control procedures for users described in those audit reports.

- Establish and follow policies and procedures to ensure data entry vendors have effective internal controls for securely processing and protecting taxpayer information. In addition, the Department should verify that data entry vendors have appropriate and effective security measures in place, that vendors are in compliance with the data protection contract provisions, and that all vendor security updates are kept current.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Concur
Contact person: Tom MacConnel, Comptroller, (602) 716-6593
Anticipated completion date: June 2009

Agency Corrective Action Plan: The Department understands that strong internal controls must extend to those vendors that perform tax processing services. Yet, funding restrictions impact the Department's ability to fully implement as robust a vendor oversight program as it would desire. The Department has taken significant steps towards this goal, however, to obtain annual assurances of the adequacy of vendor internal control systems.

Policies and Procedures
In 2008 the Department established an internal Vendor Oversight Audit Committee (VOAC). The committee expects to have completed by June 2009 a standard agency-wide process for the vendors who can provide a SAS70 internal controls report and for those who cannot. As stated in last year's response, the processes will provide four essential assurance elements to 1) track when reports or reviews are needed; 2) ensure appropriate review and documentation of results; 3) document and take corrective action if necessary and 4) follow up as needed.

For those vendors who provide an annual SAS70 report, VOAC will employ a standard internal security checklist and procedure to evaluate the findings. The process will include vendor remediation steps for unacceptable findings, final action steps for unacceptable remediation and documentation of the review outcome and actions taken. For those vendors that do not provide a SAS70 report or do not have a report for the current fiscal year, the Department will supply the vendor with a standard physical and logical internal controls survey by which the vendor will self-report on its internal controls. Any unacceptable findings will be pursued in the same manner as SAS70 report findings.

In addition, if the budget supports it, VOAC will conduct annual on-site vendor visits to evaluate physical and logical controls over confidential information.

Vendor Internal Control Systems
While the Department received in fiscal year 2009 a satisfactory SAS70 report from its electronic payment processing vendor for the annual period ending September 30, 2008, it did not receive one for its printing and mailing vendor. The Department plans to review this vendor by June 2009 when new vendor oversight procedures are finalized.

Data Entry Vendor Controls
The new vendor oversight process will include steps to ensure data entry vendors are securely processing and protecting taxpayer information. The Department anticipates all vendor oversight components to be in place by June 2009. Also, in January 2008 the Department conducted a physical inspection of the local data entry vendor but, due to budget constraints, a physical inspection for the out-of-state vendor did not occur in fiscal year 2008.

08-20
The Department of Revenue should continue to develop and implement effective controls over tobacco taxes

The Department of Revenue is responsible for licensing tobacco distributors and collecting, distributing, and reporting tobacco tax receipts. The Department collected approximately $408 million in tobacco taxes during fiscal year 2008. Therefore, it is critical that the Department maintain effective internal controls over tobacco taxes to help ensure that all taxes due to the State are collected, properly distributed, and accurately reported. While the Department began implementing controls in April 2008, it needs to develop and implement procedures to ensure the completeness of tobacco tax returns received. Further, the Department did not prepare monthly reconciliations of cigarette stamp sales to tax receipts received.

To help ensure that all tobacco taxes are collected, properly distributed, and accurately reported, the Department should:

Continue to strengthen controls to help ensure the completeness and accuracy of taxpayer returns and payment information. These procedures should include reporting and reconciling cigarette stamp sales to receipts. In addition, tobacco tax return and payment information should be restricted to essential employees. Also, manual calculations should be reviewed by an independent employee for accuracy.

- Sequentially control tobacco tax returns upon receipt to ensure all returns are recorded and accounted for.

- Reconcile all tobacco tax collections to the AFIS at least monthly. Investigate all reconciling items and make all necessary corrections.

- Improve existing procedures for collecting, distributing, and recording tobacco and use taxes from tobacco internet sales.

A similar recommendation was provided to the Department in the prior year.

Agency Response: Concur
Contact person: Steve Doyle, Special Taxes Administrator, (602) 716-6285
Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan:
Strengthening Controls
In 2008, the Department made several improvements over its tobacco tax processes to strengthen controls over tobacco tax collection, distribution and reporting. Specifically, the Department has enhanced controls by further restricting access to tobacco records, establishing independent reviews and further separating cash handling duties from deposit and distribution functions.

Ultimately, the Department’s goal is to automate the current manual process by incorporating luxury tax processing (tobacco and alcohol), into the Business Reengineering/Integrated Tax System (BRITS), thus providing a more secure and effective accounting, reconciliation and revenue distribution process. To that end, the

Department is currently modifying its cashier system to facilitate the initial steps involved in luxury tax processing. Once implemented, the tax return processing and cash handling duties currently performed in the Luxury Tax Unit will be shifted to the Process Administration Division and treated like other tax types.

It should be noted, however, that due to resource constraints, the Department cannot project when the complete automation of luxury tax processing will be complete.

Sequential Returns
In September 2008, in response to the Auditor General's 2007 audit recommendation, the Luxury Tax Unit began assigning sequential document locator numbers to all luxury tax returns. The 811 tax forms that document tobacco stamp transactions are also sequentially numbered by the License and Registration Unit to provide additional tracking controls. When the Department begins recording luxury tax payments in the cashier system, however, the system will automatically assign each return with a unique payment locator number, just as it does for the other major tax types.

AFIS Reconciliations
The Luxury Tax Unit has always reconciled tobacco tax revenue collections to AFIS for the Department's accounts. In order to reconcile tobacco tax collections to all AFIS distributions, the Department needed access to a particular AFIS report for agencies receiving tobacco revenue distributions whose access had to be granted by those agencies. In May 2008 the Department's Revenue Accounting gained access to the report and beginning with the July 2008 accounting period, the staff now conducts monthly tobacco tax collection reconciliations to AFIS for all agencies receiving distributions. When Revenue Accounting identifies a variance between AFIS and the accounting records, the Department coordinates with the agencies to ensure that the necessary corrections are made in AFIS.

Internet Sales
As soon as the Department received the Auditor General's 2007 audit recommendation regarding internet tobacco sales, Luxury Tax Unit and Revenue Accounting worked together and created a distribution procedure for funds collected from internet tobacco purchases. Luxury Tax initiated the transfer to distribute all tobacco and use tax revenues for internet sales collected between July 1, 2007 and March 31, 2008. Then beginning with the April 2008 accounting period, Luxury Tax distributed revenues on a monthly rather than annual basis. Luxury Tax and Revenue Accounting will annually review the current procedures for process improvement opportunities.

08-21
The Department of Revenue needs to test its disaster recovery plan for its BRITS system

The Department uses its BRITS to record sales and income tax transactions. Accordingly, it is critical that the Department have an up-to-date disaster recovery plan in place to ensure that BRITS can continue to operate in the event of a software or hardware failure or other system interruption. A properly designed disaster recovery plan helps ensure that proper procedures are in place to provide for continuity of operations and that electronic data is not lost in the event of a disaster. While the Department had a disaster recovery plan, the plan was last tested during fiscal year 2007. That test identified some network connectivity problems that the Department did not fully resolve. In addition, the plan was not tested during fiscal year 2008 because of difficulties encountered with scheduling the test and the Department's plans to relocate offsite data facilities for BRITS.

To help ensure continuity of operations in the event of a major system or equipment failure, the Department should test its BRITS disaster recovery plan annually. The test results, including actions the Department takes to resolve any problems identified, should be documented.

Agency Response: Concur
Contact person: Susan Silberisen, Chief Information Officer, (602) 716-6955
Anticipated completion date: Fiscal Year 2009

Agency Corrective Action Plan: In fiscal year 2008, the Department's Information Technology (IT) Division resources were focused on implementing the third and final tax type, individual income. The Disaster Recovery Plan was updated with new steps to include the corporate and individual income business processes and new Business Reengineering/Integrated Tax System (BRITS) code. The test was not completed because previous network issues experienced in 2007 between the disaster recovery site and the Department's main Phoenix facility had not been resolved. Information Technology decided to forego disaster recovery plan testing in fiscal year 2008 based on four primary factors:

1) The last tax type was not implemented into BRITS until the end of January 2008. A second critical release of BRITS was scheduled for May 2008, which left only one month to complete testing within the fiscal year. To conduct the test within such a short time period would require the use of subject matter experts across all business lines, including the Process Administration Division who was in the midst of its peak individual income tax processing period.

2) The Department was soon moving its systems to a new off-site data center service. This move constituted an extremely large IT project effort. There were not enough IT resources to work on the data center move plan and to also complete a disaster recovery test in the same time frame.

3) Disaster recovery testing was only available for a limited window of time based on the existing disaster site contract and the network issue delay. The window "closed" two months in advance of the new data center move in September 2008. Therefore, utilizing resources to test a disaster recovery plan two months before moving to the new data center, which would then require different disaster recovery plan requirements, did not make good business sense.

4) In addition, IT performed a complete disaster recovery test in November 2008 during the data center move with 100% success; results were fully documented and used to update the current Disaster Recovery Plan.

08-22
The Department of Economic Security's Division of Developmental Disabilities needs to ensure its financial statements are accurate

The Department of Economic Security and the Division of Development Disabilities' management depend on accurate financial information to fulfill their oversight responsibility and report accurate information to the Arizona Health Care Cost Containment System (AHCCCS), the public, and other interested parties. To achieve this objective, the Division needs to improve internal control over its general ledger accounting to help ensure its accounting records and financial reports are accurate and complete. The Division used spreadsheets to account for and accumulate various financial transactions for financial reporting. However, this process was prone to error. For example, auditors noted errors in the compilation process that materially misstated due from other state funds and due to other state funds financial statement line items, and various amounts in the aid to individuals expenditures financial statement note by $50,000 to $6 million. The Division adjusted its financial statements and notes for all significant errors.

This finding is considered a material weakness over financial reporting.

To help ensure that the Division's financial statements are accurate and complete, the Division should implement a system that can account for, accumulate, and accurately report all health plan financial transactions. To accomplish this, the Division should verify that amounts are transferred to the financial statements accurately and that financial statement amounts reconcile to the underlying accounting information.

A similar recommendation was provided to the Division in the prior year.

Agency Response: Concur
Contact person: Debra H. Peterson, Business Operations Administrator, (602) 542-6893
Anticipated completion date: June 2009

Agency Corrective Action Plan: The Department acknowledges that the reconciliation process between FOCUS (the Division's claim payment system) and FMCS (the Department accounting system of record) is complex and yet an integral part of the financial statement preparation. The reconciliation process will continue to be reviewed and revised to ensure that it is accurate, well documented, and complete.

Over the past year, Financial Services Administration and Division staff have worked to improve the financial statement preparation and process. These improvements have included a strengthened internal review process. Additionally, the Department has begun an initiative to automate the financial statement process and is currently developing an in-house Arizona Health Care Cost Containment System (AHCCCS) financial statement reporting application.

It is anticipated that the reporting application will be designed, developed, tested and implemented by the fourth quarter of fiscal year 2009. The application will increase the accuracy and completeness of the financial statements by reducing reliance on manual data input.

08-23
The Department of Economic Security's Division of Developmental Disabilities should follow AHCCCS approved methods to estimate its accrued long-term care costs

The Division of Development Disabilities' management is responsible for preparing accurate financial statements and complying with AHCCCS accounting and reporting requirements. As part of this objective, management should ensure that its accounting estimates for claims payable reported in its financial statements and supplementary schedules are accurate and consistently follow the methods established by AHCCCS. However, the Division has not developed AHCCCS-approved methods to identify and report institutional care and home- and community-based services (HCBS) reported but unpaid claims (RBUC) payable or estimate acute care incurred but not reported (IBNR) and RBUC claims payable. Furthermore, the Division did not follow its established methods for developing HCBS and institutional care IBNR amounts and did not obtain approval for the method used. In addition, the Division did not develop a lag schedule for ventilator services based on current patterns and actual payment information to estimate the ventilator dependent IBNR claims payable. Although the auditors determined the reasonableness of the institutional care, acute care, ventilator dependent, and other medical IBNR, the auditors could not determine the reasonableness of the Division's HCBS IBNR estimate. The Division revised its estimate and used another unapproved method. The auditors determined that the revised HCBS IBNR estimate was reasonable. Finally, the Division did not calculate the RBUCs for the HCBS and institutional care expenditures and therefore could not calculate the RBUC days outstanding.

This finding is considered a material weakness over financial reporting.

While auditors were able to determine the reasonableness of the estimates, the Division should ensure that amounts reported for claims payable in the Division's financial statements and supplementary schedules are calculated accurately and follow the methods established by AHCCCS. To accomplish this, the Division should develop and document logical estimation techniques for IBNR and RBUC claims payable to ensure consistent application. Further, the Division should periodically evaluate those techniques to help ensure they are current and effective, and are producing accurate results.

A similar recommendation was provided to the Division in the prior year.

Agency Response: Concur
Contact person: Debra H. Peterson, Business Operations Administrator, (602) 542-6893
Anticipated completion date: March 2009

Agency Corrective Action Plan: The incurred but not reported (IBNR) amounts for home and community based services (HCBS) and institutional care required additional analysis that deviated from the AHCCCS approved methods in fiscal year 2008. This reflected the stabilization of the FOCUS claims payment system and service providers' improved claim submittals, which reduced payment lags. Schedules and methodologies are being reviewed to ensure that methodologies that generate lag schedules for IBNR amounts are effective and producing accurate results. Once this process is complete, the Division will provide AHCCCS with these revised methodologies to obtain their approval by the reporting deadline for the third quarter of fiscal year 2009.

Due to changes to Arizona Long-Term Care System (ALTCS) financial reporting guidelines that are effective in January 2009, the Division will no longer be required to report claims payable for reported but unpaid claims (RBUC) days outstanding for all services and incurred but not reported (IBNR) claims payable for ventilator dependent services.

08-24
The Department of Economic Security's Division of Developmental Disabilities should strengthen computer access controls

System access controls help ensure that only authorized users have access to the Division of Development Disabilities' computer systems and sensitive data. These controls are critical in preventing or detecting unauthorized use, damage, loss, or modification of programs and equipment, and misuse of sensitive information. System access controls restrict not only physical access to the Division's systems, but also logical access to those systems. Access to the Division's computer systems should be limited to those employees authorized to process transactions or maintain a particular system.

The Division did not adequately limit logical access to its FOCUS and QMACS claims payment systems during fiscal year 2008 since it did not establish policies and procedures for computer access until January 2008. Specifically, auditors noted the Division did not always retain documentation to support that users' access was approved and did not terminate or suspend system access when there was no activity for certain users. Auditors also noted generic user accounts that were not assigned to a specific employee and could be used to make unauthorized changes to the systems. Several of these accounts included approval and update privileges. In addition, there was no audit log used to track the database administrator's activity in either system. Further, system users had incompatible responsibilities or capabilities that weren't necessary to fulfill their job responsibilities. Specifically, FOCUS users had the ability to change service rates, third-party liability waiver information, and payment addresses, and QMACS system users had the ability to issue payments and change access security privileges and eligibility. In addition, until July 2008, the help desk employees had access to all FOCUS user passwords.

To help strengthen system access controls to prevent or detect unauthorized use, damage, loss, or modification of programs and equipment, and misuse of sensitive information, the Division should follow the procedures listed below:

- Limit logical access to the Division's computer systems to authorized users.

- Retain access request forms with the supervisor's approval.

- Change an employee's system access immediately when an employee transfers from one position to another.

- Eliminate access to all computer systems promptly when an employee leaves the Division.

- Eliminate all generic user accounts and assign each user account to an individual employee.

- Document all changes to financial information made by users with significant access.

- Limit access to as few employees as possible and make sure access is compatible with each employee's job responsibilities.

- Eliminate access to all user passwords for the help desk employees.

A similar recommendation was provided to the Division in the prior year.

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

Agency Corrective Action Plan: The Division's Information Technology Application Office conducted initial reviews, in the second quarter of fiscal year 2008, of job roles and responsibilities and appropriate access to FOCUS production data. As a result of this review, policies and procedures have been changed and strengthened. These changes will help to ensure that all access is compatible with an employees' job responsibilities and prevent improper access to, or misuse of, sensitive information. In addition, these changes will ensure that only authorized users have logical access to the FOCUS system and will prevent unauthorized use, damage, loss, or modifications of programs and equipment. Specifically, the following actions have been taken to:

- Limit logical access to the Division's computer systems to authorized users.
  - In January 2008, the Division implemented policies and procedures 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.

- Retain access request forms with the supervisor's approval.
  - For both FOCUS and QMACS systems, access is granted only through the use of the J-125 process, which includes retention (hard copy or electronic) of the supervisory approval document.

- Change an employee's system access immediately when an employee transfers from one position to another.
  - For both FOCUS and QMACS systems, access is granted only through the use of the J-125 process. That access is modified upon notification of an employee transfer from one position to another within the Division or Department.

- Eliminate access to all computer systems promptly when an employee leaves the Division.
  - For both FOCUS and QMACS systems, access is granted only through the use of the J-125 process. That access is terminated upon notification of an employee leaving the Division or Department.

- 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.
  - Certain “generic” accounts are necessary in the QMACS system for Windows authentication, which is required for stored procedures and other Microsoft processes. These accounts will be evaluated to determine if alternatives exist.

- Document all changes to financial information made by users with significant access.
  - Changes made to the QMACS database, through the user interface, are logged in the database. This logging identifies the user making the change. When automated processes update QMACS tables, SQL stored procedures are utilized; the SQL account is used for database logging.
  - Changes made to the FOCUS database follow Database Administrator’s (DBA) policies and procedures that require all production releases to be recorded in a log. The procedures include use and retention of all release approval documentation.

- Limit access to as few employees as possible and make sure access is compatible with each employee’s job responsibilities.
  - For both FOCUS and QMACS systems, the additional process of terminating user accounts that have not been accessed in the previous 90 days was implemented in October 2008. This ensures that user access follows required roles.

- Eliminate access to all user passwords for the help desk employees.
  - FOCUS help desk support staff access to FOCUS production passwords (except for their own password) was eliminated, following implementation of Windows Authentication in July 2008. Due to technical limitations in the system, these employees continue to have access to user passwords for a small number of external users; however, these external users have read-only access.

  - Implementation of Windows Authentication has eliminated the need for users to enter FOCUS passwords. Thus there is no longer a need to force the users to change their passwords after initial entry.
  - The QMACS help desk sets the initial user password and cannot view the password established by the user. The QMACS help desk will reset user passwords when requested to do so by the user.

08-25
The Department of Economic Security’s Division of Developmental Disabilities should strengthen controls over computer program changes

To help ensure that an information system functions as designed, it is essential that changes to the application software be properly authorized, tested, reviewed, and approved before changes are implemented. However, the Division of Development Disabilities did not always follow its policies and procedures for QMACS system program changes. For example, of the eight program changes made during fiscal year 2008, division users did not approve six of them. In addition, for one change, documentation was not retained showing the change was tested, and that the responsibilities of developing, testing, and implementing the change were appropriately separated among employees.

To help ensure that changes to its computer programs meet user needs and objectives, and are adequately developed, thoroughly tested, and properly applied, the Division should monitor and enforce written policies and procedures to ensure that management and users:

- Authorize, review, and approve all program changes to the information systems prior to implementation.

- Retain documentation to support that program changes were authorized, tested, and approved.

Agency Response: Concur
Contact person: Debra H. Peterson, Business Operations Administrator, (602) 542-6893
Anticipated completion date: October 2009

Agency Corrective Action Plan: The Department will ensure that QMACS system changes are executed in conformance with DES Standard Development Methodology (1-38-0056). This methodology requires all program changes to document user requirements, approve testing plans which contain expected results, and requires user and/or management approval before production implementation.

Production changes to the QMACS system are executed with a request from the user. However, because of the interface with the AHCCCS reference file, it has been difficult for the user to review and approve the results prior to production implementation. The Department will develop and implement a process that reviews program changes prior to updating the AHCCCS reference file. All supporting documentation for production changes including authorization, testing, and approval will be retained.

08-26
The Department of Economic Security's Division of Developmental Disabilities needs to implement previously reported recommendations

The Division of Development Disabilities is responsible for preparing the financial statements, maintaining strong internal controls, and complying with its Arizona Long-Term Care System (ALTCS) contract. An appropriately designed internal control system should include appropriate policies and procedures to assess the effects of reported deficiencies, design an appropriate corrective action plan, and ensure that the plan is followed and implemented. However, auditors have provided detailed recommendations to the Division to correct similar deficiencies in internal controls over financial reporting and instances of noncompliance with the ALTCS contract noted during the 2002 through 2007 audits, and the Division hasn't always assessed the effects of these reported deficiencies and decided to either correct them or conclude that they will not be corrected. Specifically, the Division has not implemented the recommendations for ensuring that its financial statements are accurate, following AHCCCS-approved methods to estimate its accrued long-term care costs, and strengthening computer access controls, as described in recommendations 08-22, 08-23, and 08-24, respectively.

This finding is considered a material weakness over financial reporting.

To help ensure that the Division fulfills its responsibility to establish and maintain adequate internal controls and comply with the ALTCS contract, the Division should perform risk assessments to determine the effects of reported deficiencies, design an appropriate corrective action plan, and ensure that the plan is followed and implemented.

A similar recommendation was provided to the Division in the prior year.

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 is continuing to implement the recommendations. As previously discussed under each recommendation, the Department has been working toward implementation of each audit recommendation. Specifically:

- 08-22 – In response to last year's similar finding, Division and Financial Services Administration staff have strengthened the internal processes for the preparation of the financial statement preparation and process. Additionally, effort has begun to automate the financial statement process, which will improve the accuracy, completeness, and timeliness of the financial statements. It is anticipated that testing will be complete for implementation for use with the fiscal year 2009, fourth quarter ALTCS financial statements.

- 08-23 – Schedules and methodologies for accounting for incurred but not reported (IBNR) amounts are currently under internal review and will be submitted to AHCCCS for approval by the reporting deadline for the third quarter of fiscal year 2009.

- 08-24 – Over the past 6 months the Department has implemented the following:
    - Policies and procedures were implemented in January 2008.
    - Generic user accounts were eliminated in April 2008.
    - Production passwords were eliminated with the implementation of Windows Authentication in July 2008.

08-27
The Department of Economic Security should investigate and resolve unreconciled differences in Unemployment Insurance benefit payments in a timely manner

The Department of Economic Security's Employment Administration is responsible for processing Unemployment Insurance (UI) benefit payments to qualified recipients and disbursed more than $356 million in benefits in fiscal year 2008. Therefore, the Administration should have effective internal controls to accurately account for and control cash disbursements. However, this was not always accomplished. Although the

Administration prepared monthly reconciliations of benefit payments from its accounting records to the bank statements, it did not always investigate and correct unreconciled differences. As a result, there was an unreconciled difference of approximately $362,000 at June 30, 2008.

To help ensure that the Administration has effective internal controls that account for and control all UI benefit payments, the Administration should identify all reconciling items, investigate them, and make necessary corrections to its accounting records.

A similar recommendation was provided to the Administration in the prior year.

Agency Response: Concur
Contact person: Mark Darmer, DERS Chief Financial Officer, (602) 542-6333
Anticipated completion date: May 31, 2009

Agency Corrective Action Plan: The Department of Economic Security Division of Employment and Rehabilitation Services (DERS) identified the issues that led to the prior year unreconciled differences. The issues were related to errors in the treatment of certain reconciliation items, and those errors have been corrected. DERS now reconciles the bank statements and accounts on a monthly basis and maintains supporting spreadsheets and documentation to detail any discrepancies. DERS believes the identified issues have been corrected. Unemployment Insurance benefit payments have been reconciled as of June 2008 forward. DERS believes it is not cost beneficial to reconcile to the initial point of the unreconciled balance. DERS believes the documentation of how the unreconciled difference was arrived at and how it has been corrected from June 2008 going forward is sufficient to show that there is no unreconciled balance.

08-28
The Department of Economic Security should ensure the accuracy of its accounting records

The Department of Economic Security is responsible for the preparation of its financial statement information for inclusion in the State's Comprehensive Annual Financial Report. To achieve this objective, the Department should ensure that it accurately records financial transactions in its accounting records. However, this was not always accomplished since the Department incorrectly accrued $608,000 of fiscal year 2009 grant revenues in the general fund at June 30, 2008. This resulted in an overstatement of receivables and revenues. The Department adjusted its accounting records for all significant errors.

To help ensure that the Department has effective internal controls to properly account for and report financial information, the Department should require a supervisor to review and approve all year-end accruals.

Agency Response: Concur
Contact person: Scott Carson, Financial Manager, (602) 364-2545
Anticipated completion date: April 20, 2009

Agency Corrective Action Plan: The Department of Economic Security, Financial Services Administration, performed a draw of federal funds (document DFC12584) on the Community Services Block Grant in accordance with federal cash management procedures, without taking into account the year in which the expenditures occurred. In the future, all draws will be posted in the fiscal year in which the expenditures occurred and subsequently transferred, as necessary, to other fiscal years.

08-29
Arizona State University needs better controls over payroll expenses and its new human resources and payroll computer system.

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

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

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

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

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

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

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

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

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

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

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

This finding is considered a material weakness over financial reporting.

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

- Establish a comprehensive set of policies and procedures for monitoring and verifying payroll expenses. These policies should include detailed procedures for identifying, reporting, and recovering overpayments to employees.

- Continue efforts to investigate and recover overpayments, including those forgiven by departments and those referred to collection agencies.

- Ensure that departments are aware of and follow guidelines for verifying and approving time recorded by employees in accordance with established schedules for processing payroll.

- Improve controls over processing contract pay, additional pay, payroll corrections, and other adjustments to employees' pay to ensure their propriety.

- Provide written policies and procedures to departments for performing independent reviews of salary and other changes to ensure that they are proper and comply with university-established policies.

- Install system-automated checks to prevent unreasonable payroll transactions from being entered and processed without review and approval.

- Remove terminated employees from the system in a timely manner to ensure that they are not paid inappropriately.

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

Agency Response: Concur
Contact person: Matthew McElrath, Chief Human Resources Officer, (480) 965-9650

Anticipated completion date: Various, for anticipated completion dates see corrective action plan below

Agency Corrective Action Plan: In regard to the deficiencies noted by the auditors in finding 08-29, ASU's response and current status are as follows:

- It was noted that for a period of time after implementation, the system was unable to generate reports that departments needed to monitor and verify the accuracy of payroll expenses. This noted deficiency in not having the needed reports was rectified in the second half of fiscal year 2008. An HR expenditure report listing specific payroll expenses in relation to department budget was developed. Additionally, the following tools to assist the departments in monitoring and reviewing their payroll expenses were put into place throughout fiscal year 2009:
  - Policy FIN 203 – Org Manager Responsibilities – describes the accountability for departments to ensure their payroll expenses are accurate in accordance with their respective budgets.
  - Business Process Guide – to assist in reconciling Payroll Expenses.
  - Policy SPP 405-02 – Overpayment – addresses the process to follow in the event an overpayment has been determined.

- It was noted that there was initially centralized approval of timesheets for certain employees and not departmental approval. This noted deficiency of not having departmental approvals for all employees was rectified in the second half of fiscal year 2008. The ability for employees to change reporting of hours worked after departmental approval was removed, along with the centralized approvals of all timecards, by the end of June 2008. During the timeframe where centralized approvals were processed, an extremely low percentage, only 1.7%, of total employee hours, was paid prior to departmental approval. This was done to ensure timely payment of wages to employees during the initial system implementation. Currently, approval of an employee's time worked must be completed at the departmental level. If the department does not approve the time within the required payroll processing deadline, the un-approved time will not be brought forward for payment in the payroll system until the department submits a payroll correction to pay the employee for the subsequently approved time worked.

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

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

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

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

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

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

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

The auditors made several recommendations in conjunction with finding 08-29. ASU's response and current status of each finding are as follows:

- Establish a comprehensive set of policies and procedures for monitoring and verifying payroll expenses. The following four tools to assist departments in monitoring and reviewing their payroll expenses have been put into place throughout fiscal year 2009:
  - ○ Policy FIN 203 – Org Manager Responsibilities: Describes the accountability for departments to ensure their payroll expenses are accurate in accordance with their respective budgets.
  - ○ MyReports – HR Expenditures: Reporting of departmental payroll expenses in relation to their budget.
  - ○ Business Process Guide: Assists in reconciling Payroll Expenses.
  - ○ Policy SPP 405-02 – Overpayment: Addresses the process to follow in the event an overpayment has been determined.

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

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

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

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

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

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

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

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

- Remove terminated employees from the system in a timely manner. As previously mentioned, this recommendation was implemented during the first half of fiscal year 2009.
- Adhere to university policy by centrally maintaining employee records. As previously mentioned, this recommendation is scheduled to be completed during the first quarter of fiscal year 2010.

08-30
Arizona State University should strengthen controls over security, access, and change management for its new computer systems

Arizona State University implemented two systems, a student information system in April 2007 and, as discussed in item 08-29, a human resources and payroll system in July 2007. The systems initiate, record, process, and report financial data related to human resources, payroll, and student enrollment and financial assistance. These systems also contain sensitive and confidential information, such as employees' and students' social security numbers. Therefore, it is critical that these systems and the information they contain are secured and protected from unauthorized access, use, and modification.

However, the University did not have adequate internal controls over system security, logical access, and change management.

Security
Information technology security practices are important to protect the University's computer systems and the sensitive and confidential information which is stored on them, including information associated with over 64,300 students and nearly 25,000 faculty and staff. The University entered into an agreement with an out-of-state service organization to host its systems, thereby utilizing the service organization's facilities and hardware to run its applications. Services provided by this organization were done with the assumption that certain internal controls would be implemented by the University. However, the University did not fully implement all of the controls that were necessary to complement the service organization's controls. In particular, the University did not have a formal business continuity strategy and written policies and procedures for assessing, identifying, and mitigating security risk for its systems and had not performed a security risk assessment of these systems.

Logical Access
Logical access controls, such as those associated with identification, authentication, and authorization, are critical for protecting sensitive information and preventing and detecting unauthorized use of and modification to systems and the data they contain. Proper logical access controls help ensure that only authorized users have the ability to read, create, or modify data in a system, and that no one individual has the ability to make changes to critical data without an independent review. The University required users to have unique identifications and passwords to gain access to its human resources and payroll and student information systems. However, the University did not

install the automated lock-out features on these systems, leaving them vulnerable to unauthorized access through deliberate and persistent attempts to gain access. Further, the University did not have adequate procedures for removing users' system access after users terminated employment or transferred jobs within the University. Finally, the University did not have procedures for defining, assigning, and approving user access roles and responsibilities in the system to ensure proper separation of responsibilities. For example, auditors noted two employees who were involved in the system's development and implementation who also were able to make changes in the human resources and payroll system, such as adding employees or increasing salaries, and process payroll.

Change Management

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

This finding is considered a material weakness over financial reporting.

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

Security

- Establish a formal business continuity strategy.

- Develop and implement written policies and procedures for assessing, identifying, and mitigating security risks for the systems.

- Perform a security risk assessment of the systems, including the Web-based applications used to grant access to these systems, as mentioned in finding 08-31.

Logical Access

- Implement automated features within the systems to lock-out users' access accounts after a certain number of failed access attempts in order to reduce the likelihood of unauthorized access by potential attackers.

- Remove users' system access immediately after users terminate employment or are transferred to other jobs within the University.

- Develop procedures to ensure proper separation of responsibilities by defining, assigning, and approving user access roles and responsibilities in the systems.

Change Management

- Develop and implement written policies and procedures for making program changes to the systems. These procedures should require that program changes are documented, authorized, tested, and approved prior to implementation.

- Perform an independent review of all system changes, including those initiated by the service organization, to ensure that those changes are consistently documented, authorized, tested, and approved before being put into use.

Agency Response: Concur
Contact person: Tina Thorstenson, Senior Director, Technology & Process, (480) 290-1551
Anticipated completion date: June 30, 2009

Agency Corrective Action Plan: In regard to the deficiencies noted by the auditors in Finding 08-30, ASU's responses and current status are as follows:

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

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

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

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

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

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

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

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

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

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

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

The audit report contains several specific recommendations in conjunction with Finding 08-30.

Security

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

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

- Perform a security risk assessment of the systems, including those Web-based applications used to grant access to these systems, as mentioned in finding 08-31. This recommendation will be implemented during the fourth quarter of fiscal year 2009.

Logical Access

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

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

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

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

Change Management

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

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

08-31
Arizona State University needs to improve controls over its Web-based application used to grant access to its computer systems

The human resources and payroll and student information systems contain financial information that is reported in Arizona State University's financial statements. They also contain personal sensitive information, such as student, faculty, and staff social security numbers. One particular Web-based application is used to provide system users with access to these systems. As reported in the Auditor General's performance audit report, *Arizona's Universities—Information Technology Security*, this Web-based application was vulnerable because a combination of weaknesses could allow unauthorized access to the University's computer systems and the sensitive financial and personal information they contain. In addition, the University had not performed a security risk assessment of the Web-based portions of the payroll and student information systems as mentioned in finding 08-30.

This finding is considered a material weakness over financial reporting.

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

Agency Response: Concur
Contact person: Tina Thorstenson, Senior Director, Technology & Process, (480) 290-1551
Anticipated completion date: Completed

Agency Corrective Action Plan: In regard to the deficiencies noted by the auditors in Finding 08-31, ASU's responses and current status are as follows:

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

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

08-32
Arizona State University should strengthen controls over access, program changes, and disaster recovery for its financial accounting system

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

Logical Access

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

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

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

This finding is considered a material weakness over financial reporting.

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

Logical Access

- Monitor the activities of those employees having high levels of system access, including the ability to change data directly within the database. Further, changes to critical fields in the database should be documented and monitored to ensure all changes are properly authorized. Access to this documentation should be restricted so that employees with the ability to make database changes cannot change the documentation.

- Revoke all access privileges for employees who are placed on administrative leave immediately.

- Ensure that existing procedures for controlling and granting access to the financial accounting system provide the University with the ability to accurately identify all users having system access at a given point in time.

Program Changes

- Document, authorize, test, review, and approve program changes to the system before they are put into use.

- Ensure that an adequate separation of responsibilities exists between those who authorize, design, and develop program changes and those who put the changes into use.

Disaster Recovery

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

Agency Response: Concur
Contact person: Tina Thorstenson, Senior Director, Technology & Process, (480) 290-1551
Anticipated completion date: March 31, 2009

Agency Corrective Action Plan: In regard to the deficiencies noted by the auditors in Finding 08-32, ASU's responses and current status are as follows:

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

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

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

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

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

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

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

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

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

The auditors made several recommendations in conjunction with Finding 08-32. ASU's response and current status of each finding are as follows:

Logical Access

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

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

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

Program Changes

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

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

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

08-33
Northern Arizona University should improve controls over its computer systems

Northern Arizona University processes and stores sensitive student, financial, and personnel data on its computer systems. Therefore, the University should ensure that its Advantage accounting system functions as designed by properly authorizing, testing, reviewing, and approving modifications to the application software before implementation. Further, it is essential that physical access to the University's central computing Data Center be properly authorized. The University used a Service Order System (SOS) to track application software changes to the Advantage accounting system; however, not all changes were made through the SOS since changes could be made by multiple users without an SOS request. Further, there was no log or generated report to document all application software changes requested and made. Consequently, the University was unable to ensure that all application software changes were authorized, tested, reviewed, and approved. Additionally, the University was unable to support the listing of employees given access to its central computing Data Center.

This finding is considered a material weakness over financial reporting.

To help ensure that the Advantage accounting system reports complete and accurate information and that physical access over the Data Center is granted only to appropriate personnel, the University should establish, implement, and enforce formal written policies and procedures to ensure that management and users:

- Authorize, test, review, and approve all application software changes prior to implementation. In the event of an emergency, ensure the nature of the emergency and that any changes made are subsequently documented, reviewed, and approved.

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

- Maintain documentation to support that application software changes were authorized, tested, reviewed, and approved.

- Maintain support for the listing of those employees who have authorized access to the University's central computing Data Center and periodically review that listing to help ensure access is restricted to only essential personnel.

Agency Response: Concur
Contact person: Robert Norton, Associate Vice President for Financial Services / Comptroller, (928) 523- 6054
Anticipated completion date: June 30, 2009

Agency Corrective Action Plan: The Financial Systems Change Management Committee (FIN CMC), which oversees modifications to the Advantage system, prioritizes and approves all planned production changes. Approval for such changes is subject to proper testing by the Advantage functional user group.

Although procedures for tracking the migration of production changes have been developed using the ITS SOS system, we agree that additional controls are needed to help prevent the circumvention of these procedures. In addition, approval documentation within the SOS system can be improved to better identify planned production changes versus emergency production changes.

Within ITS, efforts are already under way to improve segregation of duties and logging of production change activity. These changes will be completed no later than 6/30/09. In addition, effective immediately, the Comptroller's Office will begin referencing FIN CMC approval actions within the SOS system for all planned production changes. Furthermore, the Comptroller's office will periodically report back to the FIN CMC on the nature of all emergency production changes.

ITS will upgrade its door access control system no later than 6/30/09. This upgrade will establish the needed control procedures that limit and monitor physical access to the central computer Data Center.

As a part of the upgrade a recertification of all physical access granted to personnel will be conducted and procedures will be put in place for maintaining support for all physical access granted.

08-34
The University of Arizona should improve its internal controls over purchasing

The University of Arizona purchases over $200 million each year from thousands of different vendors. To help ensure that the University receives quality goods and services at the best possible price, it needs to strictly follow its purchasing policies and procedures and comply with laws and regulations. The University is responsible for complying with the State's procurement laws as well as Arizona Board of Regents procurement policies and procedures. Also, the University has developed internal policies and procedures to help ensure that it complies with these requirements. However, we found that the University did not always follow its policies or had not developed adequate policies and procedures concerning competitive bidding, purchasing cards, and conflicts of interest.

Competitive Bidding

The Arizona Board of Regents' University Procurement Code requires competitive sealed bidding for purchases exceeding $50,000. Additionally, the University's policies and procedures require written quotations for purchases between $25,000 and $50,000. However, the University's procedures were not always followed. For example, auditors found that the University improperly renewed an expired maintenance contract exceeding $50,000 without obtaining the required competitive sealed bids. In addition, for a purchase that was between $25,000 and $50,000, the University obtained the required three written quotations. However, the University did not purchase from the vendor who provided the lowest quotation and did not maintain any documentation justifying why it was beneficial to buy the more expensive items.

Purchasing Cards

The University uses purchasing cards extensively and has detailed policies and procedures to help ensure that purchasing cards are used appropriately. The policies include transaction spending limits for cardholders and prohibitions on splitting purchases to avoid exceeding a cardholder's approved transaction limit. However, the University's controls were not always sufficient to detect whether expenditures were split when cardholders made purchases. For example, auditors noted one instance in which the cardholder made a purchase above the designated transaction spending limit because the vendor split the single purchase into two separate charges, each below the limit.

Conflicts-of-Interest

State law requires that the University's employees make it known when they have substantial interests, such as ownership, in vendors from which the University might purchase goods and services. In addition, university policies and procedures require employees to report any substantial interest with potential vendors by filing conflict-of-interest statements with the University's Procurement and Contracting Services Department. Those employees must then refrain from participating in or approving any purchases from those vendors. However, the University did not have adequate procedures to ensure that employees with substantial interests were not involved in approving or making purchases from those vendors. For example, auditors noted one employee who was allowed to make a purchase directly from a business of which he was part owner.

The University should strengthen its internal controls over purchasing. Specifically, the University should ensure that it implements and practices the following procedures.

Competitive Bidding

- Communicate existing university procurement policies and procedures by providing training to employees involved in the procurement process. Training should emphasize that competitive sealed bids are required for purchases over $50,000, and written price quotations are required for purchases between $25,000 and $50,000. Also, vendors providing the lowest quotation should be selected unless appropriate documentation is maintained supporting why another vendor was selected.

Purchasing Cards

- Reinforce existing university policies prohibiting the splitting of purchasing card purchases to avoid exceeding the purchasing card's transaction limit.

- Develop policies and procedures to monitor purchasing card activity to detect when splitting of purchasing card transactions occurs.

- Take corrective action, such as canceling or suspending the cardholder's purchasing card privileges, when the cardholder splits purchases to circumvent the spending limit.

Conflicts-of-Interest

- Require all current employees, at least annually, to review the conflict-of-interest statement form to determine if their current circumstances require them to revise their prior disclosure or disclose a substantial interest for the first time.

- Create a comprehensive and easily accessible list of employees who have disclosed a substantial interest in a potential vendor.

- Communicate to employees with substantial interests in potential vendors that they are required to remove themselves from any purchasing decisions or approvals with those vendors.

- Develop policies and procedures to monitor that employees were appropriately involved in the purchasing process.

Agency Response: Concur
Contact person: Kirk Ketcham, Procurement and Contracting Services Director, (520) 621-9513
Anticipated completion date: December 2008 for Competitive Bidding and Purchasing Cards, March 2009 for Conflicts-of-Interest

Agency Corrective Action Plan:

Competitive Bidding
We concur with the audit recommendation and will take appropriate action to ensure compliance with all State and ABOR procurement laws and regulations. Procurement and Contracting Services (PACS) has policies and procedures in place for all purchase order awards that require a competitive solicitation. PACS administrators will reiterate existing University procurement policies and procedures to all employees involved in the procurement process. During our monthly buyer meetings, PACS administrators will emphasize the importance of retaining proper written documentation to support vendor selection when choosing to purchase items from higher priced entities. PACS administrators will also highlight the policy on formal written competitive sealed bids which are required for purchases greater than $50,000, unless a sole source or emergency exists. An emphasis will be placed on documentation requirements for informal price quotes (via phone, fax or email) for purchases between $25,000 and $50,000.

Purchasing Cards
We concur with the audit recommendation and will actively use the "Declines Report" data to flag possible misuse. This report checks for spending patterns to detect if cardholders are attempting to make purchases over $5,000 and/or attempting to make

unauthorized purchases. This should assist PACS in determining whether any splitting, fragmenting, and/or pyramiding have occurred. When a transaction is flagged through this process PACS requires that a "Possible Non-Compliance" form be sent to the department liaison requesting justification and documentation for the transactions in question. The form must also be reviewed and signed by the director or department head.

Once all documentation is compiled it is reviewed by a PCard administrator and Assistant Director of Procurement and Contracting Services in order to determine if an actual violation has taken place. If it is determined that a violation has occurred the card will be suspended for 90 days. Notification of card suspension is sent to the department liaison and the dean, director or department head.

.

Conflicts-of-Interest

We concur with the audit recommendations and will take appropriate action to address these issues. On an annual basis, PACS will send an email to all current University employees to inform them of their responsibility to review the Purchasing Policy on Conflict-of-Interest (Policy 1.4). This policy requires that employees file a disclosure of substantial interest and/or update any existing disclosures.

The Disclosure of Conflict-of-Interest form has been revised. The signed statement is an attestation requiring that the employee not be involved in any purchasing decisions and/or approvals related to the listed vendor. Once the form has gone through a formal review process, the employee is notified whether or not a conflict-of-interest exists.

PACS has also implemented procedures to ensure that a comprehensive conflict-of-interest listing is maintained and kept current. The listing will be disclosed on the Procurement and Contracting Services Web site.

PACS internal procedures have been revised to include conflict of interest flags within the FRS vendor file (either substantial or remote). When processing requisitions, buyers are responsible for securing a vendor number from the Vendor File. At that point in time, the Buyer will identify whether the vendor has a conflict of interest designation. Should purchasing from a particular vendor be a conflict of interest, the buyer will notify the department to ensure that the employee is not involved in the purchasing decision.

The other auditors who audited the Department of Transportation reported the following material weakness:

08-35
Department of Transportation
Liabilities not accrued

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 during the fiscal year that are not paid until after year-end are reviewed based upon purchase orders in the accounts payable system. However, management did not have a control designed to capture and accrue for certain expenditures that did not have purchase orders in the accounts payable system, which also included contingent liabilities for contract litigation cases that are not covered by the State of Arizona's self-insurance program. This resulted in a material amount of liabilities not being accrued as of June 30, 2008.

Context: This finding was identified as a result of audit tests, including (1) sampling disbursements made subsequent to June 30, 2008, and determining whether those disbursements related to the year ended June 30, 2008, and (2) obtaining documentation from the State of Arizona Attorney General's office regarding the nature and status of litigation relating to the Department.

Effect: Other accrued liabilities and expenditures were inadvertently understated by $21.8 million. This resulted in management recording adjusting entries to correct this error in the June 30, 2008, financial statements.

Cause: Management did not have procedures in place to identify and accrue liabilities that did not have purchase orders.

Recommendation: We recommended that management strengthen its policies and procedures over identifying and recording potential liabilities that do not require purchase orders.

Agency Response:
Views of Responsible Officials and Planned Corrective Actions: The issue related to accrued expenditures relates to a misinterpretation of when an expenditure was incurred. In two situations, it was erroneously believed that certain expenditures did not come due until the fiscal year in which they were paid. A better understanding of what constitutes an accrued expenditure has been provided and will help in the process.

Also, Right-Of-Way staff has been directed to develop a comprehensive listing of all potential accrued expenditures and provide those to Financial Management Services for review. Ancillary to this process, a substantial number of payments that were previously made without purchase orders will now have a purchase order issued. As a further control, those purchase orders will be created with a unique prefix identifier so that they are more visible to management.

The matter relating to the status of contingent liabilities for contract litigation cases that are not covered by that State of Arizona's self-insurance program will be handled in the following manner. Financial Management Services will require that State Engineer's Office to prepare a quarterly list of all contract litigation cases. This list will be reviewed and updated with the current status of each case. At June 30, a determination will be made regarding the potential liability for each claim, and appropriate entries will be made at that time.

08-36
Arizona State University Foundation
Audit Adjustment

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

Agency Response:

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