A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Management Letter

Department of Revenue

Year Ended June 30, 2004

INTEGRITY ★ ACCOUNTABILITY ★ MAKING A DIFFERENCE

STATE OF ARIZONA
OFFICE OF THE
AUDITOR
GENERAL

Debra K. Davenport
Auditor General

The **Auditor General** is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits of school districts, state agencies, and the programs they administer.

Copies of the Auditor General's reports are free.
You may request them by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Additionally, many of our reports can be found in electronic format at:
www.auditorgen.state.az.us

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

September 6, 2005

Gale Garriott, Director
State of Arizona
Department of Revenue
1600 West Monroe Street
Phoenix, AZ 85007

Dear Mr. Garriott:

In planning and conducting our audit of the State of Arizona for the year ended June 30, 2004, we considered the Department of Revenue's internal controls over financial reporting and tested its compliance with laws and regulations that could have a direct and material effect on the State's financial statements as required by *Government Auditing Standards*.

Specifically, we performed tests of cash receipts and distributions of individual, withholding, corporate, transaction privilege, use, excise, tobacco and liquor taxes; unclaimed property liabilities; taxes receivable; tax refunds; tax refunds payable; due to local governments; payroll; and transfers.

There are no audit findings that are required to be reported by *Government Auditing Standards*. However, our audit disclosed internal control weaknesses that do not meet the reporting criteria. Management should correct these deficiencies to ensure that it fulfills its responsibility to establish and maintain adequate internal controls. Our recommendations are described in the accompanying summary.

This letter is intended solely for the information of the Department of Revenue and is not intended to be and should not be used by anyone other than the specified party. However, this letter is a matter of public record, and its distribution is not limited.

Should you have any questions concerning its contents, please let us know.

Sincerely,

Dennis L. Mattheisen, CPA
Financial Audit Director

TABLE OF CONTENTS

INTRODUCTION & BACKGROUND

In August 2002, the State contracted with a management consulting and technology services company to help improve the Department's tax collection processes and the effectiveness of its enforcement programs by developing an integrated tax information system. This new system, known as BRITS (Business Reengineering Integrated Tax System), is being implemented in three phases over the next several years. In fiscal year 2004, the Department implemented major components of the first phase by converting transaction privilege tax (sales tax) information from the old (Legacy) system to BRITS. Beginning in January 2004, the Department began processing current payments for sales taxes and individual income tax withholdings on BRITS.

During our audit of the State's financial statements, we reviewed the BRITS system to evaluate whether the Department had established adequate controls and monitoring procedures to process, record, and safeguard sensitive electronic information. As a result of our review, we noted the following areas that the Department can improve its controls over BRITS:

- Data conversion and processing controls.
- Taxpayer billings.
- Computer access controls.
- Program change controls.
- Disaster recovery plan.
- Input controls.
- Policies and procedures over computer operations.

During our audit, we made other recommendations to the Department to help improve internal controls over financial reporting and cash receipts. In addition, certain information came to our attention that has not been included in this report because of its sensitive nature. However, this information has been provided to the Department's Director.

The Department should ensure the accuracy of data recorded on BRITS

The Department uses computerized information systems to process tax collections and to store critical taxpayer information. Therefore, it is vital that the Department has appropriate policies and procedures in place to help ensure that BRITS accurately processes, records, and reports tax collections and that taxpayer information recorded on the system is accurate and complete. However, because of processing problems and data conversion problems, amounts owed to the State by taxpayers (receivables) or due from the State (payables) for individual income tax withholdings and sales taxes were not accurately maintained on BRITS. Specifically, when processing individual income tax withholdings, the system should compare payments received to the withholding return in order to determine the proper receivable or payable balance for the taxpayer. However, for the period of January through March 2005, the system did not compare at least 22,000 withholding returns filed to payments received. As a result, the Department was unable to identify or process receivables or payables attributable to those returns. For sales taxes, the Department had to convert critical taxpayer information, including receivables from its existing (legacy) systems to BRITS. However, during the conversion process, approximately 7,540 transactions, or $28 million in receivables, were either not converted or not accurately converted to BRITS.

As the Department begins to implement BRITS for other tax areas, the Department needs to ensure that all critical processes are operating effectively and that all taxpayer data converted to BRITS is accurate and complete. To help ensure that critical processes are functioning as intended, the Department should have reconciliation procedures in place to ensure the integrity of transactions processed on BRITS. Also, the Department needs to ensure the accuracy and completeness of taxpayer information converted from the Department's legacy tax systems to BRITS. The following procedures can help the Department ensure that BRITS processes tax returns and payments accurately and that taxpayer information is accurately converted from the Department's legacy systems to BRITS:

- Reconcile taxes due on tax returns filed and payments received to the accounts receivable and payable balances. All reconciling differences should be investigated and corrected. This reconciliation will help to determine whether all tax returns were processed and all tax amounts owed to the State or due back to taxpayers were appropriately recorded as receivables or payables as necessary.

- Ensure the accuracy and completeness of taxpayer information recorded on the Department's legacy systems prior to converting this information to BRITS. Once the data is converted to BRITS, reconcile control amounts, such as accounts receivable balances, from the legacy tax systems to BRITS. Investigate and correct all reconciling differences.

- Ensure that system users are involved with testing as early as possible and that an adequate amount of time is taken prior to conversion to perform testing. Correct and retest the problems that are found.

The Department should bill taxpayers in a timely manner for amounts due

The Department bills taxpayers for underpayments and notifies taxpayers of delinquent filings of required tax returns. To help maximize tax collections, it is essential for the Department to send out tax bills in a timely manner and notify taxpayers in a timely manner of delinquent filings. However, due to data conversion and processing errors encountered during the implementation of sales and withholding taxes on BRITS, the system could not produce accurate taxpayer billing statements. Therefore, the Department had to manually review and correct bills before sending them to taxpayers, which caused a significant backlog. As a result, more than 21,000 sales and withholding tax accounts, totaling almost $49.6 million in receivables had not been billed as of June 30, 2004. Further, BRITS was not equipped to produce system-generated taxpayer notices to notify taxpayers of delinquent filings of required tax returns.

To help improve collections of taxes owed to the State, the Department should implement the following internal control policies and procedures:

- Generate billing statements from the system that include applicable penalties and interest charges. Billing statements should be reviewed for accuracy and approved prior to mailing. Also, the Department should reconcile billings to the receivable accounts to help ensure the completeness and accuracy of amounts billed.

- Generate monthly statements from the system to notify taxpayers of missing returns. Statements should be reviewed for accuracy and approved prior to mailing.

- Review receivable accounts, at least monthly, and ensure that all delinquent accounts are referred to collections in accordance with department policies.

Computer access controls should be strengthened

System access controls help ensure that only authorized users have access to the Department’s computer systems. 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 Department’s systems, but also logical access to those systems. Access to the Department’s computer systems should be limited to those individuals authorized to process transactions or maintain a particular system. However, the Department did not adequately limit logical or physical access to its computer resources. For example, the Department failed to modify access privileges for an employee who transferred positions, which resulted in that employee having access rights that did not corresponded with his job assignments. Also, access to the on-site computer room was not restricted to essential employees only.

The Department should strengthen its policies and procedures over system access to help prevent or detect unauthorized use, damage, loss, or modification of programs and equipment, and misuse of sensitive information. Only authorized users should have physical or logical access to the Department’s computer systems. Also, physical and logical access should be limited to essential employees only. The Department’s written policies and procedures over access controls should include the following:

- Require supervisors to review and approve access levels granted to users to help prevent employees from having incompatible or unnecessary access rights.

- Deactivate all access rights immediately after an employee transfers positions. New access rights should only be granted after review and approval by the employee’s supervisor, ensuring access rights are compatible with the employee’s new job duties.

- Restrict physical access to computer room facilities to only those authorized individuals who need access to perform their job duties.

Since the responsibility for monitoring system access controls was spread among divisions and numerous individuals, the Department should have a Security Officer to oversee a centralized data security program. The Security Officer should be responsible for providing a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the Department’s computer-related security controls.

The Department should improve controls over computer program changes

Controlling and monitoring computer program changes are critical to ensure that computer systems function as designed. To accomplish this objective, all changes to computer programs should be authorized, prioritized, tested, and approved by users and management. However, the Department did not have procedures in place to prioritize all programming requests and monitor their status to ensure that critical changes were made in a timely manner. For example, a program change for system access was not made in a timely manner, which resulted in some users having unauthorized access to confidential and sensitive information. In addition, auditors noted several other critical program changes that had not been prioritized and assigned to applicable staff.

To help strengthen controls over computer program changes, the Department's policies should include procedures for assessing proposed program changes to prioritize change requests, ensure the efficient and effective use of IT resources, and ensure that such changes are made within required timelines. To help facilitate these processes, the Department should develop a tracking system to ensure that all program-change requests have been authorized and approved, prioritized, assigned resources, and tested, and that timelines are prescribed for each critical step in the process.

The Department should have a current and tested disaster recovery plan

A properly designed disaster recovery plan helps ensure that proper procedures are in place to provide continuity of operations and that information stored electronically is not lost in the event of a disaster or other interruption. However, the Department's disaster recovery plan was not complete, current, and had not been tested. In addition, the Department did not have adequate backup procedures. Specifically, backup data files were maintained by an outside vendor; however, the Department did not maintain an inventory listing of files provided to the vendor or monitor the vendor to ensure adequate backup files were being maintained. As a result, the Department could not be sure complete and accurate data would be available in the event of a system failure or other interruption.

To help ensure that the Department can provide for the continuity of its operations and to help prevent the loss of data in the event of a system failure or service interruption, the Department should have a well-developed, current, and tested disaster recovery plan. When completed, the Department should update and test its disaster recover plan annually. After testing, the Department should modify the plan to correct any problems to help ensure its effectiveness. The plan should include the following:

- A listing of employees assigned to disaster teams, including emergency telephone numbers.
- Employee assignments and responsibilities.
- A list of procedures for processing critical transactions, including forms or other documents to use.

In addition, the Department should prepare and maintain a current inventory listing of all back-up files and request access to the vendor's storage facility on a periodic basis to ensure adequate files are available in the event of a system failure or service interruption.

Data input controls should be strengthened

Properly designed input controls are necessary to ensure that all data entered into a computer system is accurate, authorized, complete, and input only once. The Department has developed procedures within BRITS that include flagging unusual items within the system that, based on set parameters, are incomplete, inaccurate, or exceed set range and/or dollar limits. However, these procedures will detect data input errors only after transactions have been processed and recorded on BRITS. Because of BRITS implementation and conversion problems, the Department has accumulated a backlog of review and suspense items. As a result, data input errors have not been reviewed and corrected on a timely basis. Auditors performed test work on the initial transactions entered into BRITS for individual income tax withholdings and noted that for four of 13 transactions examined, the amounts entered into the system did not agree to the input documents. While these documents were flagged as review items, the Department did not review and correct these items prior to the fiscal year end. These errors resulted in receivables being misstated by more than $450,000.

In order to ensure that information entered, processed, and stored on BRITS is complete and accurate, the Department should review all flagged and suspended items in a timely manner. Additionally, the Department should consider implementing data validation procedures as documents are first keyed into the system. The Department should analyze the most efficient and effective methods for data validation and add these controls to current and future BRITS applications. These controls may include the following:

- Keystroke verification to verify the initial entry's accuracy.
- Range, limit, and reasonableness checks to prevent fields from exceeding or falling below predetermined limits and values.

- Computer matching and control totals to ensure the data input’s accuracy.

The Department should establish policies and procedures over computer operations

Written policies and procedures aid employees in effectively performing their job duties and provide the basic framework for establishing employee accountability. They also 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. The Department has developed policies and procedures over most of its computer operations; however, the Department still needs to develop policies and procedures over the authorization and use of remote access, and firewall management and maintenance.

The Department should ensure that policies and procedures are in place to control daily operations, enhance accountability and consistency, and safeguard assets and data. The Department should establish policies and detailed procedures for the following areas:

Authorization and usage of remote access

- Preparing and maintaining a complete and current list of all authorized personnel having remote access privileges.

- Automatically disconnecting from the network after a specified period of inactivity, as determined by the Department.

- Controlling the use of security tokens, which are small hardware devices used to enhance authorized access to a network service.

- Immediately terminating remote access privileges upon employment transfer or termination.

Firewall management and maintenance

- Monitoring vendor’s firewall security bulletins.

- Backing up the firewall configuration files and retaining the backup files offsite.

- Monitoring network activity and filtering content.

- Monitoring network access controls.

The Department should ensure the accuracy of revenues and expenditures recorded on 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 accurate information is reported in the State's Annual Financial Report. Reconciling revenues and expenditures to the State's accounting system (AFIS) allows the Department to resolve any timing differences, and detect and correct input errors, such as inaccurate account codes. However, the Department did not prepare reconciliations for income tax revenues (individual, corporate, and withholding) or for payroll expenditures. As a result, auditors noted that income tax collections recorded on the Department's income tax processing system differed from amounts recorded on AFIS by more than $12 million.

To help ensure accurate and complete information is recorded on AFIS, the Department should reconcile total income tax collections recorded on its systems to the amount of income tax revenues recorded on AFIS at least quarterly. Also, the Department should reconcile its payroll expenditures recorded on the State's Human Resource Information System to those recorded on AFIS by account code after each pay period. The Department should promptly investigate and correct any differences noted.

A similar recommendation was previously provided in our Management Letter to the Department dated February 23, 2004.

The Department should strengthen controls over cash receipts

Since cash receipts are highly susceptible to potential theft or misuse, the Department should establish and enforce effective controls to safeguarded cash receipts. However, the Department did not have adequate written policies and procedures or enforce existing procedures to properly control and safeguard receipts in the Cashier Unit and Luxury Tax Division. For example, employees in the Cashier Unit were allowed to void cash receipts they prepared without a supervisor's review and approval. Also, within the Luxury Tax Division, checks were not restrictively endorsed upon receipt, and one employee of the Division opened all mail, deposited cash receipts, and prepared billings and penalty assessments. This same employee also maintained custody over the inventory of cigarette stamps.

To help strengthen controls over cash receipts, the Department should establish written policies and procedures for collecting, recording, approving, and depositing cash receipts and periodically monitor that these procedures are being followed and are operating effectively. These procedures should include the following:

Cashier Unit

- Supervisor review and approval of all voided cash receipts.

Luxury Tax Division

- Restrictively endorsing all checks immediately upon receipt.

- Separating responsibilities among employees so that no one employee opens mail receipts; deposits cash receipts; and prepares or sends out billings and penalty assessments.

- Separating recordkeeping and custodial responsibilities to ensure that cigarette stamps are properly accounted for and safeguarded.

STATE OF ARIZONA

Department of Revenue
Office of the Director
(602) 716-6090

Janet Napolitano
Governor

Gale Garriott
Director

August 26, 2005

Ms. Debra K. Davenport
Auditor General
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Dear Ms. Davenport:

The following are the Department's responses to the financial audit for fiscal year 2004 that was conducted by one of your financial audit teams at the Arizona Department of Revenue. The Department recognizes that the last six months of fiscal year 2004 were a difficult time with the initial implementation of our integrated tax system, BRITS. You will note in our responses where we have made improvements and progress in our implementation and will continue to do so as we complete the project.

Recommendation 1: The Department should ensure the accuracy of data recorded on BRITS

Department's Response: Agree

The Department understands the importance of having accurate data recorded on BRITS. The Department will make the following improvements for the implementation and conversion of Corporate and Individual Income Tax into BRITS.

The upcoming BRITS Corporate and Individual Income tax data conversion activities will utilize a planned, structured approach for system and user acceptance testing. This approach includes analysis, design, and testing of automated conversion modules; execution of mock conversions to assess data quality and refine the conversion process; identification of data purification and conversion reconciliation activities; execution of the conversion according to a detailed conversion script; and detailed reconciliation of data conversion results. In order to apply lessons learned from the TPT and Withholding tax conversions, the Corporate and Individual Income tax conversions will incorporate the following additional controls:

- Acceptance Criteria. Pre-defined acceptance criteria will be established to control and measure the data conversion process. These criteria will include elements to evaluate the success rate of data conversion from Legacy systems, and will set a minimum quality standard that must be met before production data conversion will be authorized.

- Monitoring of Conversion Issues. Conversion issues, including known issues with Legacy data will be identified and managed so that alternatives can be evaluated, and actions taken to eliminate or minimize the risk associated with the conversion issues.
- Go/No Go Decision Point. The BRITS Steering Committee (comprised of the DOR Director, Deputy Director, and those Assistant Directors with operational responsibility for the tax types being converted) will approve or disapprove the conversion for each of the remaining tax type conversions (i.e. Corporate and Individual Income tax) based upon the acceptance criteria and the list of outstanding conversion issues. If the minimum acceptance criteria have not been satisfactorily achieved, the conversion will be delayed until such time as they have been achieved.

Recommendation 2: The Department should bill taxpayers in a timely manner for amounts due

Department's Response: Agree

Currently, in BRITS, the Department is issuing billings for transaction privilege tax on a weekly basis. Billings for withholding tax are being issued but a backlog remains with a goal of being current by the fall of 2005. Included in the process of issuing billings is a manual review of a sample of billings for accuracy and an approval prior to mailing. In conjunction with issuing the billings, receivables are automatically staging to Collections for further collections activities in accordance with department policies. Although BRITS will not be capable of issuing a delinquency notice in mass until the end of 2005, delinquencies are being referred to Collections for further collections activities on a monthly basis and the specific Collector can issue a delinquency notice when working the case if he or she chooses.

Recommendation 3: Computer access controls should be strengthened

Department Response: Agree

The Department understands the importance of properly controlling access to computer resources. In October 2004, the Department created an Information Security Officer position. Over the period of October 2004 to January 2005, the IT Division assumed responsibility for BRITS data security from the project team. While the Security Officer is responsible for the centralized administration and maintenance of security processes, policies, and procedures, there are several other individuals in the IT Division who assist in the execution of specific security requests.

Since January 2005, the IT Division has conducted two Security Summit meetings to review and evaluate existing DOR security processes and procedures. As a result of these meetings, we have updated, improved, and streamlined our data security processes and tools. In addition, we are currently assembling a Security Manual which will contain all of the processes and procedures related to data security in the Department.

Limiting Logical Access

In addition, the Department's Human Resources Section will be working with the IT Division Security Officer and other employees to implement a process for notifying IT of employees changing positions within the Department and also when employees depart from the Department. The Department also conducts an annual review of data access privileges across all systems and users. The new applications implemented for the BRITS project will be included in the annual review scheduled for September 2005.

In addition to the processes discussed above, it is the Department's culture to train employees as indicated below:

- All employees and any vendor who may be exposed to taxpayer data are required to attend UNAX (unauthorized access) training required by the Federal Government. This training outlines the civil/criminal penalties for willful unauthorized access or browsing of taxpayer records.
- All employees and any vendor who may be exposed to taxpayer data receive specific taxpayer Confidentiality training provided by the Department.
- All employees and any vendor who may be exposed to taxpayer data are required to review and sign a Confidentiality agreement annually. The agreement states that employees will not access accounts that are not directly related to their job function. The agreement also states that the employee is responsible for reporting to their supervisor any inadvertent access to unauthorized accounts.

Limiting Physical Access

Access to the computer room at the Department is secured by a proximity card reader that requires a badge for access. The Department and/or Department of Administration (DOA) must specifically grant access privileges to an individual for him/her to gain access to the computer room at the Department. Vendors accessing the computer room are escorted by an authorized Department employee.

Historically, a formal review of all personnel with access to the computer room was conducted annually and access was revoked if deemed inappropriate. In the future, we will increase the frequency of these reviews to a quarterly cycle.

Recommendation 4: The Department should improve controls over computer program changes

Department Response: Agree

The Department understands the importance of prioritizing system requests to ensure timely response to critical changes.

In September 2003, the BRITS project team implemented a web-based tool to record, track, prioritize, and assign requests for work related to the BRITS project and systems. The System Investigation Request (SIR) portal is used to record and track software defects, requests for enhancement, training needs, security changes, report requests, documentation updates, etc.

In January of 2004, after the first release of BRITS went into production, SIRs were prioritized for completion within each Division – Collections, Taxpayer Services, etc. The BRITS project team managed the work efforts but work queue priority was determined by individual Divisions.

Over the period of October 2004 to January 2005, the IT Division assumed responsibility for BRITS data security from the project team. Beginning in January 2005, security related SIRs are now assigned to designated personnel for evaluation. Currently, requests for user adds/changes/deletes are typically resolved within 1-2 business days. SIRs related to system-wide security changes typically require additional research and are completed based on the priority assigned to the request.

In March of 2005, the IT Division assumed responsibility for management of the BRITS production systems and implemented a formal process for reporting and prioritizing BRITS system issues on an agency-wide basis. A report containing a complete inventory of outstanding production SIRs is produced monthly. The report is reviewed by all Divisions to identify priority items.

The BRITS Steering Committee, which is comprised of the Director, Deputy Director, and Assistant Directors from each of the operational Divisions, meets to discuss and agree on the agency-wide priorities. Once the SIRs are prioritized, the requested changes are estimated and completed based on the complexity of the request and availability of staff.

Recommendation 5: The Department should have a current and tested disaster recovery plan

Department Response: Agree

The Department understands the critical nature of securing the information vital to its on-going operations. The Department has a comprehensive Business Continuity plan for the agency and the disaster recovery plan elements for the BRITS production systems were incorporated into that plan in early 2005. The Department's Business Continuity includes such information as identified in the Auditor General report.

The BRITS production systems are housed at the AT&T data center in Mesa, Arizona. The responsibility for the backup and recovery of these systems belongs to the Department's third part vendors - AT&T and Accenture Technology Infrastructure Services (ATIS). These vendors were selected to house and support the Department's production servers specifically because of their managed data center expertise and familiarity with the BRITS system technologies and architecture.

The Department has reviewed the vendors' disaster recovery plans and determined they meet or exceed the approved statewide standards. A disaster recovery test of the BRITS production systems is scheduled for August 2005.

As the Department's vendors, AT&T and ATIS are responsible for securing and maintaining the physical inventory of all backup files. The Department has reviewed the vendors' procedures and determined they meet or exceed the approved statewide standards. Since the BRITS system went into production in January 2004, we have had occasion to request file restores from backup tapes – these restores have been completed without any data loss. However, the Department will incorporate procedures for auditing the AT&T and ATIS backup file inventory and processes into existing procedures.

Recommendation 6: Data input controls should be strengthened

Department Response: Partially Agree

The Department does agree with the finding that in the past data input errors were not being reviewed and corrected on a timely basis. During the initial implementation of BRITS and the newness of the system to our employees, incorrect items were posted to taxpayer's accounts. However, review items would have stopped any incorrect billings or refunds from going out to the taxpayer and would also have given the Department another opportunity to correct any potential errors. Currently, the process discussed below is in place in BRITS for both transaction privilege tax and withholding tax.

Keystroke verification to verify the initial entry's accuracy

Under ideal circumstances we would agree with this recommendation. However we do not have the human or financial resources to double key the high volume of documents received. Presuming we had the budget to do this, there would not be enough time and outside help available to meet the service levels the public has come to expect from the Department. The Process Administration Division processes approximately 100,000 transaction privilege tax returns per month, 100,000 withholding tax returns per quarter, 60,000 corporate returns per year, and 2,300,000 individual income tax returns per year. Given the volume of returns processed annually, the Department determined that the best method to ensure accuracy and remain cost effective was to establish an error resolution process in which the BRITS system assisted to identify any potential errors after the data was keyed by employees of the Data Entry Unit.

Range, limit, and reasonableness checks to prevent fields from exceeding or falling below predetermined limits and values

The department does agree that these checks are prudent. However we do not have these checks on the data entry process because of the high volume of returns that are keyed and the limited resources we have to key these returns. In order to ensure accuracy, once the return information is transmitted to the BRITS system, the information will be run through several suspense rules that will identify when there are errors in the data. Those returns with errors will not post to the taxpayer's account until a Department Error Resolution Unit employee reviews the return and makes any applicable corrections. With the implementation of BRITS, the Department gained an additional opportunity to identify potential errors. The process in BRITS is called Review Item work. Once again, the Department has identified several rules that return data is evaluated against to determine if another review of the information is necessary prior to a billing or refund being sent out to the taxpayer. If the return data meets any of the criteria in the rules, a review item is set on that return. No billing or refund will be sent out to the taxpayer until a Review Item Unit employee reviews the return and makes any applicable corrections.

Computer matching and control totals to ensure the data input's accuracy

The department does agree that control totals would help ensure data accuracy and this has been discussed within Processing management in past years. However it was determined that the time spent running calculator tapes would exceed the benefit of the gains in accuracy. We rely on our back end suspense and review process to catch processing errors.

Recommendation 7: The Department should establish policies and procedures over computer operations

Department Response: Agree

Remote Access

The Department implemented Virtual Private Network (VPN) connectivity in 2001. The VPN solution allows employees to access the Department's computer resources remotely in a secure manner. The VPN project was reviewed and approved by the Internal Revenue Service Technical Audit Group prior to implementation.

In order to gain remote access to the Department, an employee must receive approval from his/her supervisor and attend a two hour class on telecommuting. Once the training is complete, the Assistant Director of Administrative Services forwards the IT Division an email evidencing approval for the remote access.

Upon receipt of the approval, the Department issues the approved employee an AZDOR laptop and a CRYPTOCard (secure token) and adds the employee to an authorization security list. The CRYPTOCard prevents the use of static, weak, or easily cracked passwords, providing a very high degree of confidence that only authorized users get access to protected resources.

An employee accessing the Department's computer resources remotely will automatically be disconnected from the network after a Department-determined specified period of inactivity.

In addition, the Department's Human Resources and Payroll Sections will be working with the IT Division Security Officer and other employees to implement a process for notifying IT of employees changing positions within the Department and also when employees depart from the Department.

In July 2005, the Department updated the Computer Use and Confidentiality policy that addresses modem use and telecommute access for employees. All employees are required to review and sign the policy annually. The Department will combine the existing telecommute policy from the Employee Handbook and the existing internal procedures into one formal policy that encompasses all procedures surrounding remote access for employees.

Firewall Management and Maintenance

The Department follows industry standard best practices, such as those identified by the Auditor General report, related to management and maintenance of firewall configurations. In order to further ensure the security of computer resources, the Department also engages Cisco, an industry recognized leader in network tools and security, to conduct an annual network penetration audit. The CISCO audit pinpoints potential network vulnerabilities and the Department immediately resolves all concerns identified. The Department will formally document the policies and procedures in place related to firewall management and maintenance.

Recommendation 8: The Department should ensure the accuracy of revenues and expenditures recorded on AFIS

Department Response: Agree

The Department understands the importance of reconciling the income tax revenues from the applicable tax system to AFIS. It is the Department's goal to do so. The legacy tax systems did not provide ability for the Department to accomplish this task. One of the main revenue accounting requirements of BRITS is to provide the ability to reconcile between the two systems. Income tax revenues are made up of revenue that is associated with withholding tax, corporate income tax, and individual income tax. Currently, the Department is testing the requirements in BRITS to reconcile withholding tax revenue. The ability to reconcile Corporate and Individual income tax revenue will come when those tax types are converted and implemented in BRITS.

The Department understands the importance of reconciling its payroll expenditures from HRIS to AFIS. However, during the last six months of FY04, HRIS did not provide the applicable information to allow this task to be accomplished. Beginning in the second quarter of FY05, HRIS did provide the information and the Department began to reconcile its payroll expenditures to AFIS.

Recommendation 9: The Department should strengthen controls over cash receipts

Cashier: Employees were allowed to void cash receipts they prepared without a supervisor's review and approval.

Department Response: Agree

The Department understands the importance of having strong controls over its cash receipts. The Department has modified its written polices and procedures to require a supervisor's review and approval of voided cash receipts.

Luxury Tax: Restrictively endorse all checks immediately upon receipt.

Department Response: Agree

All checks received by the Luxury Tax division are endorsed upon receipt and deposited the same day. If checks are received after the deposit has been made, these checks are now endorsed and locked up for the following day's deposit. In order to ensure that all luxury tax checks are now restrictively endorsed immediately upon receipt, all checks received by the Cashier Unit, for sales of luxury tax stamps, will now be endorsed upon receipt by that unit.

Luxury Tax: Separate responsibilities among employees so that the employee who collects cash receipts does not also record and deposit the receipts or prepare and send out billings and penalty assessments.

Department Response: Agree

The division has instituted procedures which provide for the separation of duties so that the responsibilities of opening mail receipts; depositing cash receipts; and preparing or sending out billing and penalty assessments are not handled by one employee. There are currently three separate employees who are each responsible for one of these actions. On occasion, due to absences, it may be required for the individual who is responsible for sending out billings and penalty assessments to also deposit cash receipts. However, another employee will have opened the mail and recorded the payment prior to this individual receiving the payment for deposit.

Luxury Tax: Separate record keeping and custodial responsibilities to ensure cigarette stamps are properly accounted for and adequately safeguarded.

Department Response: Agree

While most of the stamp process has strong control points built in, we do recognize that the current procedures are not adequate with respect to the return of stamps, and the subsequent destruction or restocking of the returned stamps. Going forward, the division will have two individuals sign off on the receipt of the returned stamps and a certification of destruction will be created which will be signed by the facilities employee when the stamps are destroyed.

Thank you for the opportunity to respond to this report. The Department is very appreciative of your staff's understanding and professionalism during this financial audit process.

Sincerely,

Gale Garriott,
Director

cc: File