

ATTACHMENT C
STATE OF COLORADO



DEPARTMENT OF REVENUE
State Capitol Annex
1375 Sherman Street, Room 409
Denver, Colorado 80261
Phone (303) 866-3091
Fax (303) 866-2400

Bill Ritter, Jr.
Governor

Roxanne Huber
Executive Director

June 14, 2010

Sally Symanski, State Auditor
Office of the State Auditor
200 East 14th Avenue
Denver, Colorado 80203

Dear Ms. Symanski:

The Department of Revenue is in receipt of your letter dated April 1, 2010, requesting a status update on the recommendations noted in the *Colorado Integrated Tax Architecture Project – Phase I Implementation, Information Technology Audit, September 2009*. Attached please find the Department's update on the actions taken to implement the recommendations noted in the audit.

If you have any questions regarding this information or the Department's implementation of the recommendations, please contact me at (303) 866-5610.

Sincerely,

A handwritten signature in cursive script that reads "Roxanne Huber".

Roxanne Huber
Executive Director

Attachment

Recommendation No. 1:

The Department should perform a supervisory review of severance tax refunds initiated and approved by the same tax examiner for the period of November 3, 2008 through March 11, 2009. Additionally, prior to the deployment of future CITA phases, the Department should rigorously test GenTax to identify and correct potential segregation of duties issues.

Response: Agree

Current Status: Implemented

Original Response:

As mentioned in the State Auditor's narrative contained in the bullet above, this issue was identified on March 4, 2009. A solution request was submitted and the correction was made to GenTax on March 11, 2009. Our research concludes that the finding is indeed accurate and the solution implemented on March 11, 2009 makes it impossible for an examiner who adjusts the account resulting in the refundable credit from also being able to provide any level of approval for that same refund. Additionally if a refund request is generated manually then that user is also prevented from participating in approval. We have identified accounts where a combination of edits and approval appear on the same account and we are in the process of completing a review. To date we have found no indication of error or fraud.

Updated Status, May 2010:

As mentioned above, a correction has been put in place which systematically prevents an initiator of a refund from also performing the needed approval. Furthermore, every account that fit this condition has had a supervisory review performed upon it and those reviews revealed that the refunds were issued properly and no problems were discovered. This recommendation has been fully satisfied and is completed.

Recommendation No. 2:

The Department of Revenue should improve controls over the data migration process for future CITA phases by:

- a. Establishing and maintaining sufficient, competent, and relevant evidence to demonstrate that legacy data reconciles with the data migrated to GenTax as of the go-live date and that any record deletions are fully documented. Reconciliations and deletions should be reviewed by a supervisor.
- b. Requiring business owners to assess and formally accept data migration results through physical signoffs.
- c. Recording and documenting user access privileges to the data during each stage of the migration process.

Office of the State Auditor CITA Phase I Audit
Implementation Status Update
Department of Revenue

- d. Requiring either the IT security or internal audit staff to periodically review user access privileges during the data migration process to ensure access levels are appropriate.
- e. Obtaining the active involvement of the Department's internal audit staff during all stages of the data migration process, including reviewing the adequacy of the data migration plan and the accuracy and completeness of the data.

Response 2a: Agree

Current Status: Implemented

Original Response:

The Department agrees that establishing control totals regarding legacy data is an important reconciling feature in the data migration and conversion process. The legacy system does not provide the necessary discrete control total reports that would be preferable. Instead, we will utilize reports generated by independent IT programming resources to establish control totals which will be compared with the extracted, cleansed and converted data into GenTax to ensure accuracy and completeness. The criteria and the process related to reconciliations and deletions will be evaluated by a supervisor but the volumes involved in converting income tax data preclude an account by account review. We will document the criteria used for data cleansing and the data verification process and will confirm the use of this criteria.

Updated Status, May 2010:

While the existence of legacy control total reports remains an issue for the project, we are cognizant of the matter and are taking steps to provide a sufficient, competent and relevant demonstration that the data converted into the new system represents the entire population of data intended to be converted from legacy systems.

Response 2b: Agree

Current Status: Implemented

Original Response:

We agree with this recommendation and we have implemented a process to secure user formal acceptance of data migration through a physical sign-off which will be obtained for the migration of Phase 2 taxes to GenTax prior to the cutover date of November 2, 2009.

Updated Status, May 2010:

This recommendation has been fully implemented.

Response 2c: Agree

Current Status: Implemented

Original Response:

Office of the State Auditor CITA Phase I Audit
Implementation Status Update
Department of Revenue

The project will formalize and document the process for granting user access privileges for each stage of data migration. However it should be noted that during Phase 1 controls were in place to limit user access to all stages of the data extract, cleansing and conversion processes. We simply did not have the ability to completely document who had access at each stage, but access was indeed limited.

Updated Status, May 2010:

The process for granting, recording and documenting user access privileges to the data during each stage of migration is described in the CITA Infrastructure Security and Change Control documentation. In addition a record has been kept of who had access to the conversion environment during the Phase 2 data migration.

Response 2d: Agree

Current Status: Implemented

Original Response:

Department management, as part of the process referenced above, will determine and authorize the appropriate user access privileges. Internal Audit will verify the process is in place and the control is working as intended.

Updated Status, May 2010:

The Department management has determined the appropriate user privileges for extract cleansing and migration of data into the new system. The system Internal Auditor has been involved in this process and has reviewed user access privileges.

Response 2e: Agree

Current Status: Implemented

Original Response:

The Department hired a System Internal Auditor in June 2009 and this position will work with the CITA team in reviewing the adequacy of the data migration plan and how it addresses the validation of the data.

Updated Status, May 2010:

The Department has hired an Internal Auditor whose primary focus is automated systems. He has reviewed the data migration plan and has been involved on the CITA project as a primary responsibility. This recommendation has been satisfied.

Recommendation No. 3:

The Department of Revenue should work with the Governor's Office of Information Technology to mitigate the risks to CITA by:

- a. Continuing to work with OIT to advocate for the funding necessary to complete CITA.
- b. Developing a written knowledge transfer plan to ensure that the loss of key CITA personnel is addressed prior to project completion.
- c. Working with OIT to identify ways to increase IT resources for CITA.
- d. Identifying the specific reasons for user resistance to GenTax and developing strategies for improving overall user acceptance. At a minimum, the Department should increase its communication to GenTax users and provide more job-specific training.
- e. Developing a separate business and IT process alignment plan or incorporating specific business alignment activities in the current CITA Project Implementation Plan, including steps for updating business and IT policies and procedures to correspond with the changes required by GenTax.

Response 3a: Agree

Current Status: Implemented

Original Response:

The CITA project is the most important project within the Department of Revenue and perhaps the State of Colorado. As such, it is incumbent upon the Department of Revenue, the CITA project and OIT to advocate for the need to continue to fund this critical project.

Updated Status, May 2010:

Funding for Fiscal Year end 2011 has been secured for the project.

Response 3b: Agree

Current Status: Partially Implemented

Estimated Completion: June 2012

Original Response:

The project team has identified the need for a comprehensive knowledge transfer plan to be of the highest importance. It is true that the Department of Revenue is faced with significant employee turnover in key areas. The CITA project itself represents an opportunity to review and document procedures which will, as a byproduct, improve knowledge transfer within the agency. This is an ongoing effort which will be completed prior to implementation of the final phase of the project.

Updated Status, May 2010:

Office of the State Auditor CITA Phase I Audit
Implementation Status Update
Department of Revenue

The initial activities associated with developing the formal comprehensive knowledge transfer plan have begun. Current DOR IT developers are taking an active role in both configuring Phase 3 of the project and in the role of production support making user requested changes and corrections to the existing system configuration. This practical experience provides necessary understanding of the GenTax system. This knowledge will become the foundation of the comprehensive knowledge transfer plan. This recommendation will be fully implemented prior to the completion of the final phase of the project.

Response 3c: Agree

Current Status: Partially Implemented

Estimated Completion: Ongoing

Original Response:

The project will work with OIT in an effort to identify ways to increase IT resources assigned to the CITA project.

Updated Status, May 2010:

The project continues to work with OIT on a number of different issues, including provision of supplemental resources for the CITA project. The response from OIT has been encouraging. If a specific resource need is identified we will not hesitate to approach OIT with the goal of obtaining a resource with the necessary skill set from existing state OIT employees.

Response 3d: Agree

Current Status: Partially Implemented

Estimated Completion: Partially Implemented with ongoing communication efforts.

Original Response:

The project management team has begun the process of enhancing our change management and communication plans. There is a normal human tendency to resist change, especially if that change is substantial and directly impacts an individual. It is the project management team's belief that any initial resistance can be attributed to this normal human reaction. Research suggests that, the cycle of adaptation to change, is much like the grieving process. There is an initial period of denial followed by a period of grieving and finally there is acceptance of the new environment. However it is important to be proactive in combating user resistance. Accordingly, we are developing job specific user training that will facilitate easier understanding of the new GenTax system and we will increase the frequency and the depth of our communications with the user community.

Updated Status, May 2010:

The project developed job specific user training for Phase 2 of the project. This training was well received and has helped users more quickly adapt to the new system. We will continue this strategy for all future phases by developing and delivering job specific training to users. Furthermore the project

Office of the State Auditor CITA Phase I Audit
Implementation Status Update
Department of Revenue

contracted for the creation of a communication plan intended to improve both internal and external communication about the project. We believe more frequent and more meaningful communication will positively impact both user and customer acceptance of the new system. As more users gain proficiency in the GenTax application they serve as early adopters and knowledge experts who help the organization transition efficiently to the new system.

Response 3e: Agree

Current Status: Partially Implemented

Estimated Completion: Ongoing

Original Response:

As mentioned in the response above, we have embarked upon a process of improving our change management plan. This process will include aligning the business and IT organizations in a manner that leverages the capability within the GenTax system.

It is important that all business and IT policies and procedures be updated to correspond to the changes precipitated by the introduction of the GenTax system; however it is important to note that GenTax is a new tool for the user community but most, if not all of the essential work remains the same. We process remittances, capture data, process tax returns, create and review edits, audit taxpayer returns and records and manage the accounts receivable. Phase 1 involved the implementation of small taxes. It was our desire to roll out the system, get the tool in the hands of the users, give them experience using this tool and only then develop formal written procedures governing the day to day activities of the user community. The business procedures must be written by the business units themselves because they are the only ones who are in a position to fully understand and utilize the system functionality. The process of updating operating procedures, by necessity, lags the implementation of each phase.

Updated Status, May 2010:

The process of updating work procedures is an important but time consuming process. The business users have rewritten most procedures necessary to support the new system and work continues towards the objective of rewriting all user procedures. The initial work of identifying roles and responsibilities for IT employees has been completed and process alignments and procedural changes will be updated as needed. This recommendation will be fully implemented prior to the implementation of the last phase of the project.

Recommendation No. 4:

The Colorado Office of Cyber Security (OCS) should continue to assist the Department with the security of all CITA system and network components throughout all project phases to ensure that security controls adhere to State Cyber Security hardening policies and industry best practices. The OCS should provide written notice to the CITA Project Team of any recommended changes. The Department of Revenue should not formally accept future phases of the CITA Project until all recommended changes

Office of the State Auditor CITA Phase I Audit
Implementation Status Update
Department of Revenue

have been made and the OCS certifies the security of the underlying IT infrastructure, including servers and network components.

Current Status: Partially Implemented

Estimated Completion: June 2012

Original Response:

The configuration and hardening of servers and server software are important considerations. The Department will work with OCS to ensure that servers utilized in the CITA project meet the required standards; however, the Department does not believe it has the authority to "not formally accept future phases of CITA" until the recommended changes have been made and OCS certifies the underlying IT infrastructure. Acceptance of future phases of CITA is dependent upon satisfaction of contractual requirements by Fast Enterprises. If Fast Enterprises successfully delivers according to contractual obligations, the Department is compelled to accept future phases and compensate the vendor according to the terms of the contract.

Updated Status, May 2010:

The Department's Information Security Officer has been and will continue to work with the Colorado Office of Cyber Security throughout all phases of the project to ensure that project related security controls adhere to the State Cyber Security hardening policies and to industry best practices.

Recommendation No. 5:

The Department of Revenue should strengthen its general computer controls by:

- a. Immediately addressing all deficiencies in the GenTax server configurations we identified in the audit and provided to the Department under separate cover.
- b. Implementing controls over the GenTax change management process. The Department should require that Fast Enterprises change its policies and procedures so that the same person making code changes is not authorized to move those changes into production. Additionally, the Department should require Fast Enterprises to implement an independent, supervisory review of code changes to ensure that only authorized changes were made to GenTax.
- c. Immediately disabling all accounts belonging to terminated users, including network accounts and implementing the Fiscal Year 2008 recommendation to improve communication between the human resources section and the IT security administrator to ensure that user access is revoked for terminated employees going forward. Additionally, the Department should begin taking disciplinary action against all employees that fail to comply with established user access procedures. Failure to notify Department IT security staff of terminated users or to terminate users upon receiving notice should be immediately escalated to the Department's executive management and appropriate disciplinary action taken.

Office of the State Auditor CITA Phase I Audit
Implementation Status Update
Department of Revenue

- d. Documenting GenTax user profiles, or combinations of profiles, that are appropriate for different system users on the basis of job responsibilities. This documentation should be shared with the supervisors of GenTax users and used as the basis for establishing user profiles.
- e. Documenting profiles or profile combinations that provide escalated system privileges, including the establishment of compensating controls where appropriate.

Response 5a: Partially Agree

Current Status: Partially Implemented

Estimated Completion: Ongoing

Original Response:

The Department agrees with this finding, and has begun to address the deficiencies identified in the audit. In particular, all of the deficiencies identified as "high risk" have been closed already, and we expect to have accomplished further improvements by the Legislative Audit Committee meeting in late September. Some of the lower risk items will only be addressed as the Department is able to complete its migration from the old Microsoft NT environment to the new Active Directory environment, an ongoing process that will not be completed before fiscal year end.

Updated Status, May 2010:

As mentioned in our original response, the Department has already addressed all of the high risk deficiencies. Some of the lower risk items can only be addressed after the Department completes its migration from Microsoft NT to the new active directory environment. The plan is to have that migration completed by July of 2010. Any low risk items remaining will be resolved after that date.

Response 5b: Partially Agree

Current Status: Implemented

Original Response:

The team leads for each section are responsible for reviewing the code produced by the developers that work for them. Additionally only team leads are allowed to approve migration requests to production. Due to resource constraints and to efficiently leverage the team leads experience, team leads can also make code changes and can subsequently request migration of that code to production. Fast has agreed that migrations requested by a team lead where the team lead also made the code changes will be approved by a different team lead. This will be a procedure that we will audit for compliance on a regular basis.

Updated Status, May 2010:

Fast Enterprises has agreed to not allow code migration into production without a review by an independent team lead who was not involved in writing the code change.

Office of the State Auditor CITA Phase I Audit
Implementation Status Update
Department of Revenue

Response 5c: Partially Agree

Current Status: Implemented

Original Response:

Work will begin immediately on disabling the accounts. To address the timely removal of employee's access, the Department is in the process of implementing a streamlined notification process. Disciplinary action will be considered and utilized when appropriate.

Updated Status, May 2010:

The project, through its Steering Subcommittee, has implemented a process whereby appointing authorities who have employees authorized to access GenTax review the list of their employees on a monthly basis to make sure user access levels are correct and that all terminated employees have their system access removed. The process has been in place for several months and is working well. A streamlined notification process for avoiding future occurrences has been in production and is being used across payroll, IT, security administrators, Office of Human Resources, etc.

Response 5d: Partially Agree

Current Status: Partially Implemented

Estimated Completion: August 30, 2010

Original Response:

It should be noted that current user profiles are determined based upon the work unit to which an employee is assigned and their level of responsibility/authority. Therefore it is possible for employees with the same job classification title to have substantially different user access profiles. The Department understands the purpose for this recommendation and we agree that benefits can accrue from its implementation; therefore, we will document the user profiles and combinations of profiles and share this documentation with supervisors and GenTax users so that there is a broad understanding of what type of access is granted to different members of the user community.

Updated Status, May 2010:

The project has gone through the process of designing and documenting a series of user profiles and combination of profiles that are specific to different positions within the Department. We expect to have all of our environments: development, staging and production updated with the new profiles by the end of August 2010.

Response 5e: Partially Agree

Office of the State Auditor CITA Phase I Audit
Implementation Status Update
Department of Revenue

Current Status: Partially Implemented

Estimated Completion: August 30, 2010

Original Response:

The Department will document user access profiles which provide escalated system privileges and any associated compensating controls.

Updated Status, May 2010:

The new process of creating user profiles and combination of profiles also encompasses provision of access to escalated system privileges. This entire process will be fully implemented by the end of August, 2010.