Colorado Integrated Tax Architecture Project –
Phase 1 Implementation
Department of Revenue

Information Technology Audit
September 2009

**OFFICE OF THE
STATE AUDITOR**

LEGISLATIVE AUDIT COMMITTEE
2009 MEMBERS

Representative Dianne Primavera
Chair

Senator David Schultheis
Vice-Chair

Senator Morgan Carroll
Representative Jim Kerr
Representative Frank McNulty

Representative Joe Miklosi
Senator Shawn Mitchell
Senator Lois Tochtrop

OFFICE OF THE STATE AUDITOR

Sally Symanski
State Auditor

Dianne Ray
Deputy State Auditor

Jonathan Trull
Kerri Hunter
Legislative Audit Managers

Lillian Adams
Julie Chickillo
Pooja Tulsian
Manjula Udeshi
Legislative Auditors

The mission of the Office of the State Auditor is to improve the efficiency, effectiveness, and transparency of government for the people of Colorado by providing objective information, quality services, and solution-based recommendations.

STATE OF COLORADO

Sally Symanski, CPA
State Auditor

OFFICE OF THE STATE AUDITOR
303.869.2800
FAX 303.869.3060

Legislative Services Building
200 East 14th Avenue
Denver, Colorado 80203-2211

September 3, 2009

Members of the Legislative Audit Committee:

This report contains the results of an information technology audit of the Department of Revenue's management of the Colorado Integrated Tax Architecture project, Phase 1 Implementation. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Department of Revenue and Governor's Office of Information Technology.

Glossary of Terms and Abbreviations

CITA Feasibility Study – Approved by the General Assembly in Fiscal Year 2005 to assess the most efficient and cost-effective way to upgrade the Department of Revenue's primary revenue and tax systems.

CITA Staff – Department of Revenue and Fast Enterprises staff assigned to the CITA project to develop and maintain the GenTax application to DOR's needs and specifications.

Computer Application or Application – a computer program or set of programs that perform the processing of records for a specific function. Examples of computer applications include Microsoft Office, Microsoft Excel, COFRS, and GenTax.

Colorado Integrated Tax Architecture Project or CITA – a $56.4 million endeavor undertaken by the Colorado Department of Revenue to replace multiple legacy tax systems currently used to collect, account for, and distribute state and local taxes.

COTS/MOTS – Commercial-Off-the-Shelf/Modify-Off-the-Shelf computer application. Refers to existing computer software available for sale to the general public. COTS/MOTS applications can typically be customized to meet the specific needs of the user.

DOR, Department – Department of Revenue, the state department responsible for managing the state tax system and collecting tax revenue.

EGC – Executive Governance Committee, established by the Governor's Office of Information Technology to assist OIT with the oversight and governance of certified IT projects.

General Computer Controls – controls that relate to the environment within which computer-based applications are developed, maintained, and operated. The objectives of general computer controls are to ensure the proper development and implementation of computer applications and the confidentiality, integrity, and availability of program and data files.

GenTax – the proprietary, integrated tax processing software developed and owned by Fast Enterprises LLC. GenTax is also referred to as the base system and is the primary component of CITA.

IT – information technology.

IT Infrastructure – all information technology assets (hardware, software, data), components, systems, applications, and resources.

IV&V – Independent Validation & Verification. An independent contractor hired to substantiate that an IT system development process, overall project management, and deliverables were developed, performed and delivered in accordance with the project contract.

OIT – Governor's Office of Information Technology, created to secure and protect IT assets; optimize spending for IT decisions, projects and technology; and effectively manage IT projects.

This page intentionally left blank.

Colorado Integrated Tax Architecture Project – Phase 1 Implementation

Purpose and Scope

In September 2007, the Department of Revenue (Department) officially kicked off the Colorado Integrated Tax Architecture project (CITA). CITA is a $56.4 million IT project designed to replace the Department's existing legacy tax systems and aging IT infrastructure with a modern, integrated and taxpayer-centric software known as GenTax. CITA is one of the most expensive IT projects ever undertaken by the State, and once implemented, the new system will support one of the State's most critical functions: the annual collection and distribution of nearly $10 billion in state and local tax revenue.

Large-scale IT projects like CITA are fraught with challenges and, if not managed properly, can end in failure. In fact, studies indicate that the failure rate for IT projects often exceeds 50 percent. The State of Colorado has experienced several large IT project failures in the past five years, including the Department of Labor and Employment's $24.2 million Genesis Project which was cancelled prior to completion. Studies show that project failures typically occur because of poorly defined project scopes and objectives, lack of senior management support, lack of project management experience, poor contract monitoring, insufficient user involvement, incorrect or inappropriate technology choices, and/or lack of knowledge about changing technologies. State IT project failures result in wasted taxpayer money and agency resources, loss of taxpayer trust, and reputation damage for the State.

Because of the importance, cost, and risks associated with CITA, the Office of the State Auditor will conduct an audit of the implementation of each of the five phases of the CITA project. The Phase 1 information technology audit evaluated whether Phase 1 was completed on schedule and on budget. Further we assessed whether Fast Enterprises, the State's principle contractor, was complying with contract requirements and providing key deliverables on schedule. In addition, we performed testing to determine if the GenTax system was delivered with the features and functionality not only contracted for but also necessary to efficiently and effectively administer the State's tax system. We also assessed risks to future CITA phases and reviewed the general computer controls over the GenTax application related to severance taxes. As part of the audit we reviewed policies and procedures; interviewed key personnel; examined system configurations; reviewed computer-generated reports; surveyed GenTax users, Fast Enterprises

staff, and Department project and IT staff; and used automated computer security evaluation software to test security of the Department's network, servers, and databases related to GenTax. We also interviewed project management and cyber security staff at the Governor's Office of Information Technology (OIT) and reviewed project governance committee meeting minutes related to CITA.

The audit work was performed from December 2008 through July 2009 and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Summary of Findings

According to the CITA Independent Validation, and Verification (IV&V) contractor and OIT, the Department, in cooperation with Fast Enterprises and other contractors, successfully implemented Phase 1 of CITA. Our audit found that:

- The implementation of GenTax for severance and estate taxes and property tax credits was completed on schedule, on budget, and according to the project scope of work.

- For severance and estate taxes and property tax credits, GenTax is operational and contains all required features and functions.

Although the CITA IV&V contractor and OIT determined that Phase 1 was successfully implemented, we identified changes to GenTax that are necessary to ensure proper segregation of duties. Additionally, we identified problems with the Department's and Fast Enterprises' management of the data migration process. Specifically, due to the lack of sufficient and appropriate evidence, we were unable to verify the completeness and accuracy of the converted data. We also identified areas where improvements could be made to decrease the risk of project failure during the remaining four phases of CITA and identified weaknesses in the Department's general computer controls over the GenTax system.

The remainder of the report is divided into two sections. The first section provides descriptive information about CITA, including information about the project's history; management and oversight structure; and schedule, budget, and expenditures. The second section discusses our specific findings and recommendations.

Section I - Project Background

Between October 2004 and June 2005, the Department conducted a feasibility study known as the CITA Feasibility Study (Study) to assess the most efficient and cost-effective way to upgrade the Department's primary revenue and tax information systems. Based on the results of the Study, the Department issued a Request for Proposal for a Commercial-Off-the-Shelf/Modify-Off-the-Shelf (COTS/MOTS) solution. A COTS/MOTS solution is an existing and proven computer system that can be configured to meet the user's (in this case the Department's) specific needs. In 2007 the Department contracted with Fast Enterprises' to purchase and implement the GenTax software for CITA.

GenTax is an integrated tax processing software package designed to support multiple taxes. GenTax also provides support for most administrative functions typically found in government revenue agencies. As of June 2009, Fast Enterprises has deployed the GenTax software in 15 other states.

The Department's overall goals for CITA are to:

- Consolidate multiple, antiquated, disparate tax processing systems into a single, contemporary, integrated, taxpayer account-centric system that incorporates business best practices for state tax administration.

- Implement Fast Enterprises' COTS/MOTS GenTax application in discrete stages over a four-year period beginning in March 2008 and concluding in June 2012.

- Comply with statewide IT architecture, security, hosting, and disaster recovery standards established by OIT.

CITA Project Management and Oversight

CITA is managed and overseen by several different agencies, individuals, and committees. With the passage of Senate Bill 08-155, the management of state agency information technology resources and projects is centralized under OIT. However, because CITA was underway prior to the State's IT consolidation, the Department continues to maintain primary responsibility for day-to-day project management and oversight. As discussed below, OIT provides high-level project accountability, oversight, and support through its executive governance committees. The figure on page 6 outlines the overall project management and reporting structure for CITA. We describe each individual's and committee's management and oversight responsibilities below.

- **State Chief Information Officer (State CIO).** With passage of Senate Bill 08-155, the State CIO is responsible for the management, administration, and oversight of state agency information technology resources and projects. The State CIO is appointed by and answers to the Governor. The State CIO is the administrative head of OIT.

- **OIT Finance Executive Governance Committee (EGC).** As part of the State's IT consolidation efforts, the State CIO created executive governance committees (EGCs) to provide high-level accountability for state IT projects. The CITA Project Management Team is responsible for reporting monthly to the Finance EGC. The Finance EGC includes senior-level IT and business staff from other state agencies and is chaired by the State CIO.

- **Project Steering Committee.** The CITA Project Steering Committee is comprised of the Department's executive director, chief information officer, and key business managers; the CITA Project Sponsor (described below); Fast Enterprises project management staff; and the CITA Project Manager (described below). The CITA Project Steering Committee is responsible for setting overall project direction and providing high-level project oversight and accountability. The CITA Project Steering Committee meets monthly.

- **Independent Validation & Verification (IV&V) Contractor.** The IV&V contractor is hired by the Department to provide periodic independent assessments of CITA. The IV&V contractor is responsible for reporting the results of the assessments to the State CIO, Finance EGC, and the CITA Project Steering Committee.

- **Project Sponsor.** The CITA Project Sponsor is a senior executive from within the Department's taxation division. The Project Sponsor is responsible for championing the project throughout the Department, obtaining the necessary financial and human resources, and setting and articulating the vision for CITA from the tax administration business perspective. The Project Sponsor is a member of the CITA Project Management Team and the CITA Project Steering Committee.

- **CITA Project Manager.** The Department contracted with AdvanTech LLC to provide professional project management services for CITA. As required by the contract, AdvanTech LLC has assigned a full-time, experienced project manager and project management analyst to CITA. Both the project manager and analyst are onsite at the CITA location. The

CITA Project Manager is responsible for preparing and maintaining the project management plan; monitoring project deliverables; escalating project disputes to the Project Management Team; managing the CITA implementation plan; providing day-to-day oversight of project activities; identifying, clarifying, and managing project issues; and preparing and providing project status reports to the Department and OIT.

- **Project Management Team.** The CITA Project Management Team consists of the Project Sponsor, Department CIO, Fast Enterprises project management staff, and CITA Project Manager. The Project Management Team is responsible for the day-to-day management of the project, including establishing and monitoring work plans, managing resources, and communicating project results to key stakeholders. The Project Management Team meets weekly.

- **Project Team.** The CITA Project Team consists of Department and Fast Enterprises staff. Project team members are grouped into functional areas such as revenue accounting, collections/audit, conversion, and training. A senior staff person from both the Department and Fast Enterprises oversees each functional area. The CITA Project Team members are responsible for carrying out the day-to-day tasks necessary for project implementation.

CITA Project Management Structure

Source: Department of Revenue.
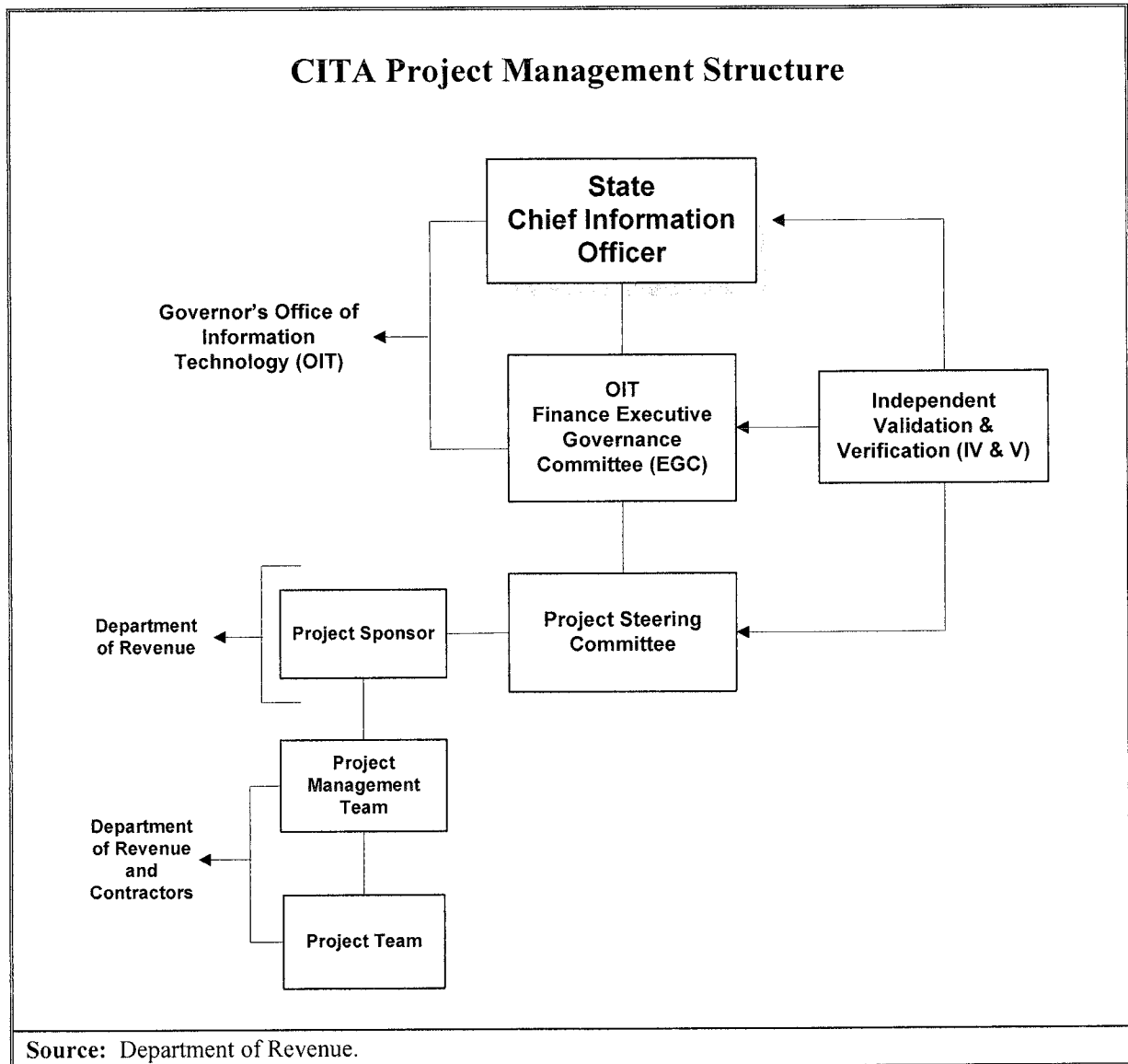
CITA Schedule, Budget, and Expenditures

CITA is a multi-phase project scheduled to be implemented from March 2008 through June 2012. In total, CITA consists of six phases, numbered 0 to 5. Phase 0 primarily consisted of project site development and overall project planning and preparation. For budget purposes, Phase 0 included the purchase of the initial GenTax license, annual maintenance and support, the first installment of the project facility, and the development of the CITA Project Plan. Phase 1 consisted of the rollout of GenTax for severance and estate taxes and property tax credits. The remaining four phases encompass the rollout of specific tax types, for example, individual and corporate income taxes will roll out during Phase 2. As shown in the following table, Phase 1 taxes (severance and estate taxes, and

property tax credits) went into production on November 3, 2008, as originally scheduled.

	Comparison of CITA Project Schedule to Actual Implementation By Phase As of June 30, 2009		
	Tax Types	Scheduled Implementation	Actual Implementation
Phase 0	Site build & Project Preparation	February 2008	February 2008
Phase 1	Estate, Severance, Property Tax Credit	November 2008	November 2008
Phase 2	Income Tax	November 2009	
Phase 3	Sales and Use, Wage Withholding, Fuel and Vehicle	November 2010	
Phase 4	Taxpayer Access Point, Discovery, Bankruptcy	September 2011	
Phase 5	Food Service, Gaming, Tobacco, Alcohol, Public Utilities Commission, Off-Highway	June 2012	
Source: Office of the State Auditor analysis of the CITA Implementation Plan and other data.			

The total projected cost of CITA is $56.4 million, as shown in the table below. More than half of this amount will be spent on acquiring the professional services necessary to complete CITA. To date, the Department has used contractors to provide professional services related to network design, application development, data conversion, independent validation and verification, and project management. The Department has also set aside approximately $2.7 million or 5 percent of the total project budget as a contingency for potential cost overruns. The remaining funds are budgeted for software licenses, building lease payments, server hardware, user hardware, training, and travel. The CITA budget does not include the personnel costs of state staff working on the project or incorporate costs incurred by other agencies such as OIT.

CITA Budget		
Cost	Budget	Percentage of Total
Professional Services	$29,300,000	52%
Software Maintenance	10,000,000	18
Software Licenses	6,000,000	11
Building Lease	5,300,000	9
Project Contingency	2,700,000	5
Server Hardware	2,400,000	4
User Hardware	400,000	<1
Training	300,000	<1
Travel	7,000	negligible
Total	$56,407,000	100%
Source: Department of Revenue.		

As of June 2009 the Department had expended approximately $15.8 million or about 62 percent of the total CITA appropriations through Fiscal Year 2009. As part of the $15.8 million expended on the project, the Department spent $4 million for the initial GenTax license during Phase 0.

Comparison of CITA Appropriations to Expenditures In Millions As of June 30, 2009			
	Expenditures	Actual	Percentage
Fiscal Year 2008	$17.6	**$8.2**	**47%**[1]
Fiscal Year 2009	$7.8	**$7.6**	**97%**
Fiscal Year 2010	$7.5		
Fiscal Year 2011	$10.7		
Fiscal Year 2012	$8.6		
Fiscal Year 2013	$4.2		
Total	**$56.4**		
Source: Office of the State Auditor analysis of the CITA budget and expenditure data.			
[1] The Department changed the project schedule, moving the largest tax types from Phase 1 to Phase 2. The Department continues to roll unexpended funds forward and anticipates spending the majority of these unspent funds in Fiscal Year 2010.			

Section II - Phase 1 Implementation

Although no statewide standards exist at this time, the following industry-proven rating categories are generally used by state agencies, OIT, and IV&V contractors for analyzing the success and/or failure of IT projects:

- **Green Light or Project Success.** The project is completed on time and on budget, with all features and functions initially specified.

- **Yellow Light or Project Challenged.** The project is completed and operational but over budget, over the time estimate, and offers fewer features and functions than originally specified.

- **Red Light or Project Failed.** The project is cancelled at some point during the development cycle.

Based on the above criteria, OIT concluded that Phase 1 of CITA was a success. Specifically, throughout Phase 1, OIT's Finance EGC consistently gave CITA a "Green Light," indicating the project was on schedule, on budget, and within scope. Additionally, the Department contracted with Wyant Data Systems, Inc., a professional IV&V firm, to perform an independent assessment of CITA's progress. Wyant Data Systems, Inc. reported in its July 2009 CITA IV&V Assessment that:

> The Phase 1 implementation of GenTax for severance, property tax credit, and estate taxes was successful and on time and on budget. The software works well and most users are satisfied.

Additionally, according to the Department's contract with Fast Enterprises, the State must formally accept each CITA phase by confirming that the contractor delivered all contract deliverables and met all specified success factors. As part of the acceptance process, GenTax must operate for a minimum of four consecutive weeks with no high-level defects. High-level defects are defined as defects that prevent the system from functioning and for which either no workaround exists or a workaround exists but the cost to repair the defect is significant. Also according to the contract, GenTax and the supporting infrastructure must meet specific performance metrics related to transaction processing speed. Failure to meet the specified performance metrics is considered a high-level defect.

On March 6, 2009, the Department officially accepted Phase 1. Prior to accepting Phase 1, the CITA Project Manager confirmed and reported to the Department that (1) Fast Enterprises had provided all contract deliverables, (2) GenTax

contained the required features and functions and was consistently meeting specified performance metrics, and (3) GenTax had been operational for at least four consecutive weeks with no high-level defects.

While Phase 1 is an important milestone for the State, we identified deficiencies related to internal controls over CITA that must be addressed in order to ensure that data are secure, data integrity is maintained and the State receives full value from this major investment.

Improvements to GenTax

Although GenTax contained the features and functions specified in the Department's contract with Fast Enterprises, we identified specific application-level controls that should be addressed for the modules implemented in Phase 1 and for future phases. Specifically, as part of the audit, we tested a sample of severance tax returns and refunds processed by GenTax following the completion of Phase 1. We identified the following problem with the GenTax application:

- Of the 60 severance tax returns sampled, 20 (or 33 percent) were initiated and approved by the same person. GenTax was not initially programmed to prevent the same person from both initiating and approving the same transaction. This lack of system edit increases the likelihood of employee fraud as well as incorrectly issued refunds. The Department identified this problem on March 4, 2009 and requested that GenTax be programmed to prevent the same person from initiating and approving a tax refund. System programmers implemented the required change into production on March 11, 2009. Although the Department identified this problem and has added the necessary changes to GenTax, Department management has not done a retroactive, supervisory review of those refunds initiated and approved by the same tax examiner.

To address the problem we identified, the Department should perform a supervisory review of all severance tax refunds initiated and approved by the same tax examiner within GenTax. Depending on available resources, the Department could perform the review on a sample basis. If significant problems are identified, all such refunds should be reviewed. We also recommend that prior to deployment of future CITA phases the Department's business users should rigorously test GenTax to identify potential segregation of duties issues. Problems should be corrected prior to moving GenTax into production.

(Classification of Finding: Control Deficiency – See Appendix A)

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.

Department of Revenue Response:

Agree. Implementation date: September 30, 2009.

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.

Data Migration

Data migration is the process of transferring data between computer systems. Data migration typically includes five phases: design, extraction, cleansing, load, and verification. In the design phase, staff map data in the old system to the new system and develop methods of extraction that capture all relevant data and, if necessary, reformat the data to meet the requirements of the new system. For example, the date field in the old system may use the format *yy / mm / dd* and the new system requires *mm / dd / yyyy*. During the cleansing phase, data are cleaned (modified or deleted) to improve data quality, eliminate redundant and obsolete information, and to match the data requirements of the new system. Finally, after the data are cleaned and loaded into the new system, business owners use testing methods to verify the completeness and accuracy of the data.

Phase 1 required CITA staff to migrate data from several of the Department's legacy systems to GenTax. As part of the audit, we reviewed the CITA staff's methodology for data migration and found the approach to be reasonable. However, we were unable to verify or substantiate the completeness and accuracy

of the converted data due to a lack of sufficient and appropriate evidence. This was due to the fact that CITA staff did not retain a snapshot of the data from the "go live" date (November 3, 2008). We were therefore unable to compare the go live data with the source legacy data. Further, although CITA project staff generated reconciliation reports during the data migration process, the reports were incomplete and did not provide an appropriate level of assurance regarding data integrity. Finally, CITA staff did not maintain system-generated reports identifying those staff who had access to state tax data throughout the migration process. Therefore, we could not verify that only appropriate and authorized staff had access to the data. Furthermore, neither the Department's internal audit staff nor the IT security staff reviewed user access during the data migration process to ensure access to protected tax data was appropriate.

Further, industry best practices require that business owners accept responsibility for the accuracy and completeness of the data during the migration process. We found that Department business staff were not entirely clear on their roles and responsibilities during the data migration process and thus did not physically sign off that they had verified the completeness and accuracy of the migrated data.

Because we could not verify the accuracy and completeness of the data migrated to CITA at the transactional or taxpayer account level, we performed an analytical review of severance tax transactions both prior to and after cutover to GenTax. We analyzed analytics only for severance taxes because, of the three tax types included in Phase I, severance taxes generate the greatest amount of revenue. Based on our analytical review, we found that the volume and dollar amount of severance tax transactions and related account fund balances appeared reasonable and closely matched those for accounting periods prior to cutover to GenTax. Although the severance tax account balances appear to be materially correct, we cannot conclude on whether or not the data migrated to GenTax are complete and accurate. Errors in individual taxpayer accounts may exist that this type of analytical review would not detect.

Controls over data migration are critical for ensuring that complete and accurate data are loaded into GenTax. Additionally, controls are necessary to ensure that CITA staff cannot perpetrate fraud during the data conversion process by adding, deleting, or modifying state tax records. For future phases of CITA, the Department should improve its controls over the data migration process. At a minimum, the Department should maintain readily available, electronic copies of the data extracted from the legacy system and loaded into GenTax as of the go-live date. The data extracted from the legacy systems and loaded into GenTax should be fully reconciled to the data in the legacy systems, and any record deletions should be documented and thoroughly explained by CITA staff. The reconciliations and any record deletions should be reviewed by a supervisor. The Department should also require its business owners to verify the completeness and accuracy of the data during the migration process and to provide a physical signoff signifying acceptance of the data. We also strongly encourage that the

Department's internal audit staff be actively involved during the data migration process to ensure that appropriate controls are in place, access to sensitive data is restricted, and data loaded into GenTax are complete and accurate.

(Classification of Finding: Significant Deficiency – See Appendix A)

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.

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.

Department of Revenue Response:

a. Agree. Implementation date: December 2009.

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.

b. Agree. Implementation date: November 2009.

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.

c. Agree. Implementation date: December 2009.

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.

d. Agree. Implementation date: December 2009.

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.

e. Agree. Implementation date: October 2009.

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.

Risks to CITA Project Success

As previously discussed, the State has seen several large IT projects fail. One of the most important factors in delivering a successful project is identifying and managing risk. For IT projects, risk is defined as anything that could have a negative impact on the project's outcome. To ensure project success, the Department should periodically identify and quantify risks to the CITA project and develop risk response plans to deal with those risks most likely to occur and posing the greatest potential negative impact.

OIT has established a common methodology or framework for quantifying risks to state IT projects. The methodology categorizes and rates risks by both the probability that a risk will occur and the impact or potential harm if the risk event does occur. OIT's ratings for probability and impact range from "high" to "low." A high probability and impact rating indicates that a risk is both likely to occur and will catastrophically impact the project. OIT recommends that departments with risks rated as high-high or high-medium have a risk mitigation plan. Low risks provide no immediate threat to project success and therefore do not require a separate risk mitigation plan.

We reviewed the CITA Project Management Team's risk assessment and response documentation and found that it complies with OIT IT project standards. Specifically, in March 2008 the CITA Project Management Team completed a risk assessment and mitigation plan for Phase 1 that identified risks to the project and quantified the probability of the risk occurring and the impact that the risk would have on overall project success.

As part of the audit, we independently evaluated and quantified risks to CITA's success in future phases. We interviewed business users, members of the CITA Project Management Team, and project staff; surveyed CITA project team members and GenTax users; reviewed system-generated reports; analyzed the Department's policies and procedures; and considered the potential impact to the project should the risk occur. Our analysis indicates the Department faces significant risks that could have an adverse effect on the CITA project. As the table below shows, we identified one risk with a high-high rating and five risks with a high-medium rating. We describe these specific risks following the table. In the section following the table, we discuss each risk and what action the Department has taken to address it.

Colorado Office of the State Auditor Risk Analysis of CITA			
Risk Description	**Probability**	**Impact**	**Overall Risk Score**
Insufficient Funding for Future Project Phases	High	High	High-High
Loss of Key Personnel	High	Medium	High-Medium
Lack of Skilled IT Staff for GenTax	High	Medium	High-Medium
Internal User Resistance to Change	High	Medium	High-Medium
Business Processes Not Aligned with GenTax	High	Medium	High-Medium
IT Processes Not Documented or Aligned with GenTax	High	Medium	High-Medium
Source: Office of the State Auditor analysis based on information obtained from the Department of Revenue.			

- **Insufficient Funding for Future Phases.** The General Assembly appropriates funding for the CITA project on an annual basis. Although the Department has secured funding for the CITA project through Phase 3, state budget deficits imperil funding for the final phases. Failure to implement GenTax for all tax types would have long-term financial and operational implications for the Department and would threaten the overall success of the project. Specifically, if GenTax is not fully implemented, the Department would need to support several tax systems that rely on vastly different technologies. For example, the Department would require IT staff skilled in both COBOL for legacy systems and Visual Basic programming for GenTax. The Department would also need different business processes and procedures based on the tax type being processed and whether the legacy system or GenTax was being used. This would likely result in significant redundancies and inefficiencies, as well as higher operating costs. Further, the early termination of CITA would result in the Department's failure to achieve the project's primary goal of consolidating "multiple, antiquated, disparate tax processing systems into a single, contemporary, integrated, taxpayer account-centric system that incorporates business best practices for state tax administration." The Department is aware of this risk and is actively working to secure funding for the final phases of CITA.

- **Loss of Key Personnel.** During our interviews, we learned that many key state staff working on CITA plan to retire either prior to the final phase of CITA or upon project completion. Soon-to-retire Department staff include project managers; program developers; network administrators; system administrators; division controllers; and business tax managers, supervisors, and other staff. The loss of these critical staff without an appropriate transfer of knowledge would have detrimental effects on

CITA's overall success. The CITA Project Management Team has not yet identified loss of key personnel as a risk to the project or taken steps to address this risk by creating a knowledge transfer plan.

- **Shortage of Appropriately Trained IT Staff for GenTax.** The Department lacks sufficient IT staff trained in the newer programming languages needed to support the GenTax development requirements for Phase 2. Additionally, Department IT staff are not currently trained to provide ongoing support and maintenance for those tax types migrated to GenTax in Phase 1. Several issues limit the number of sufficiently trained Department IT staff. First, the Department's IT staff are trained and experienced at application development and program maintenance in a mainframe environment using more than 30-year-old programming languages such as COBOL and aging database systems such as ADABAS. The GenTax software is based on new programming languages and operates in a Microsoft Windows environment using relational database management systems. The learning curve for Department IT staff has been and will continue to be steep.

  Second, Department IT staff have not had sufficient opportunities to participate in the ongoing development of GenTax. Due to the complexity of the data conversion process, Department IT staff have been required to spend the majority of their time developing extract scripts to move the data from the legacy mainframe systems to GenTax. As a result, Department IT staff are not receiving the hands-on experience necessary to learn the new system. Fast Enterprises estimates that it takes a programmer one to two years to become proficient with GenTax, making it crucial that Department IT staff be brought up to speed during the final three years of the project.

  Finally, the Department is struggling to provide the necessary IT resources to simultaneously support the existing legacy tax systems and develop the GenTax system. The Department is aware of this issue and has worked to bring on additional IT staff by contracting with recently retired state IT staff. However, CITA project management reports that more IT staff are needed for Phase 2 due to the size and volume of individual and corporate income tax filers. Further, contracting with retired IT staff is not an effective long-term strategy.

- **Internal User Resistance to Change.** The Department is facing significant user resistance to GenTax. Many of the users we interviewed and surveyed are unhappy with GenTax and do not feel prepared to use the new system. Although some user resistance is common with system changes, significant user resistance can hamper overall project success and undermine the efforts of project management. The Department has

worked diligently to address user concerns and has provided ongoing GenTax training and support. However, user resistance continues and should be anticipated for future phases.

- **Business Processes and Procedures Not Aligned with GenTax.** As part of the audit, we reviewed the Department's policies and procedures for processing severance taxes and found that the Department has not updated its policies and procedures to align with GenTax. GenTax is more than a new IT system; it represents a new way of doing business for the Department. GenTax will not be fully successful as an overall project or be accepted by users until the Department's business processes and procedures are revised to align with GenTax.

- **IT Processes Not Aligned with GenTax.** Similar to business processes, the Department has not yet aligned its IT processes and procedures with GenTax. For example the process of moving code from development into production does not adhere to State Cyber Security Policies. Similar to GenTax users, Department IT staff do not feel prepared to take over ongoing maintenance and support of the recently implemented GenTax IT infrastructure. Considering the imminent retirement of key Department IT staff, it is critical that IT processes and procedures be updated to align with GenTax.

Steps Necessary for Reducing Risks to CITA

As identified by our audit and CITA project staff, there are significant risks to the project's future success. The CITA Project Management Team should take specific steps to mitigate the six high probability risks, including at a minimum:

- Continuing to work with OIT to advocate for the funding necessary to complete CITA.

- Developing a written knowledge transfer plan to address the loss of key personnel. The plan should align with specific CITA milestone dates and require physical signoff by project managers and functional team leads upon completion. The CITA Project Management Team should also develop a mechanism to track knowledge transfer and make adjustments to the plan to ensure that state staff are sufficiently trained and knowledgeable to support ongoing GenTax operations by the conclusion of CITA in 2012.

- Working with OIT to identify IT professionals in the State with the appropriate skill set that could be temporarily moved to the CITA project to either support GenTax development activities or backfill positions vacated by Department IT staff moved to CITA.

- Pinpointing 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 user training. To date, GenTax users generally feel that they have not been sufficiently trained to effectively perform their jobs in GenTax. For example, one user interviewed told us GenTax is "like having a new car but not knowing how to drive it." Lack of job-specific training appears to be a key factor to internal user dissatisfaction with GenTax. User training is also important to ensure that staff can assist taxpayers with problems they may encounter.

- Developing a separate business and IT process alignment plan or incorporating specific business alignment activities into the current CITA Project Implementation Plan. Business and IT process alignment should be conducted in parallel with the rollout of specific tax types in CITA.

- Updating business and IT policies and procedures to correspond with the changes required by GenTax.

(Classification of Finding: Significant Deficiency – See Appendix A)

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.

Department of Revenue Response:

a. Agree. Implementation date: Ongoing.

> 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.

b. Agree. Implementation date: June 2010.

> 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.

c. Agree. Implementation date: June 2010.

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

d. Agree. Implementation date: Ongoing.

> 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.

e. Agree. Implementation date: Ongoing by phase. Complete June 2012.

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.

Governor's Office of Information Technology Response:

a. Agree. Implementation date: Immediate and ongoing.

The Governor's Office of Information Technology (OIT) commits to continue assisting the Colorado Department of Revenue (DOR) on securing the necessary funding to finish the CITA project. Successful implementation of the CITA system is a high priority for OIT, and we have partnered with DOR in the past to convey to the Governor's Office of State Planning and Budgeting and to the General Assembly the importance of adequate and continued phased funding. We fully intend to continue these activities through the completion of all CITA phases.

c. Agree. Implementation date: Immediate and ongoing.

The Governor's Office of Information Technology (OIT) agrees to actively work with the Colorado Department of Revenue (DOR) to pinpoint skill sets and resources that would benefit the CITA project. Recently, OIT conducted a statewide skills assessment to identify IT

staff expertise and centers of excellence across the Executive Branch agencies, and this effort has enabled us to expeditiously deploy resources from one agency to another to fill skill gaps in order to address and resolve urgent and critical IT-related issues. However, until Executive Branch IT personnel are budgetarily transferred to OIT, cross-agency assignments can only occur on a temporary and short-term basis. Pursuant to Senate Bill 08-155, OIT anticipates that the personal services transfer will occur in Fiscal Year 2011.

General Computer Controls

General computer controls are controls that relate to the environment within which computer-based applications are developed, maintained, and operated. The objectives of general computer controls are to guarantee the proper development and implementation of computer applications and ensure the confidentiality, integrity, and availability of program and data files. Although Fast Enterprises and other contractors are working with the Department to implement CITA, the Department maintains responsibility for implementing and maintaining general computer controls over its tax systems, including GenTax. We evaluated the Department's controls over GenTax and identified weaknesses related to server configuration, change management, and user access management. The specific areas of weakness are described below.

Server Configuration

State Cyber Security Policies and industry best practices require that the servers supporting critical systems be hardened or configured to protect sensitive information. Server hardening includes removing or changing all guest accounts and default passwords, disabling non-essential services, and setting system parameters to mitigate potential attacks. Using specialized, automated tools, we tested the configuration of the primary servers supporting GenTax, including application and database servers and the Department's primary domain controller. We identified significant weaknesses in the servers' configurations that make GenTax and the Department's other systems vulnerable to attack and compromise. Due to the sensitive nature of these control deficiencies, we provided our specific findings and recommendations to the Department under separate cover.

For future phases of the CITA project, we recommend that the Colorado Office of Cyber Security (OCS) perform automated testing of newly added servers and network components supporting the deployment of GenTax. The OCS should certify the security of the servers and network components and make appropriate recommendations to the Department. Recommended changes should be made by

the Department and contractors prior to the final acceptance of the contract deliverables. Additionally, the Department should immediately address the above-mentioned deficiencies we identified in the GenTax server configurations.

Change Management

Industry best practices require that duties be segregated to prevent security risks from occurring, such as a programmer writing malicious code and moving it into production. Application change management best practices require that a person other than the programmer who made the code changes review the code to ensure that no unauthorized changes were made. Additionally, the programmer changing the code should not have the authority and security permissions to move the code from the development and testing environments into production. For the GenTax system, we reviewed a sample of 25 application changes and found that 18 (or 72 percent) of the changes were created by the same programmer who moved the code into production. We discussed this with CITA project management staff and learned that Fast Enterprises allows its senior programmers to both change GenTax code and move the code into production. This increases the risk of errors going undetected and creates the risk that CITA staff could perpetrate fraud by making unauthorized changes to GenTax.

To mitigate potential risks, we recommend that the Department require Fast Enterprises to implement appropriate controls over the GenTax change management process. A staff person other than the programmer making the code changes should be required to independently review the changes to ensure no unauthorized changes were made. Further, the programmer making the changes should not be authorized to move the code into the production environment.

User Access

User access to GenTax and the Department's network must be tightly controlled and managed because of the critical and sensitive nature of the information processed by the application and transmitted over the network. State Cyber Security Policies require state agencies to provide users only with the least amount of access necessary to perform their job duties and to establish procedures to ensure that IT security administrators are immediately notified when an employee resigns or is terminated. Additionally, state agencies are required to immediately remove all system access belonging to terminated employees.

During our testing for the Statewide Single Audit for Fiscal Year Ended June 30, 2008, we had found that the Department's controls for managing user access were inadequate. At that time, we recommended that the Department develop and implement a formal user access management program, including periodically producing and reviewing a list of current system users and linking the human

resources and user access management functions. The Department agreed to implement the recommendation by December 31, 2009.

For this audit, we reviewed the Department's controls for managing user access to GenTax and evaluated the Department's progress in implementing last year's recommendation. Overall, we found that user access management continues to be a problem at the Department. At the time of our review, we identified 34 network IDs belonging to terminated employees. These 34 IDs were active an average of 218 calendar days after the owners' termination dates. Active network IDs belonging to terminated employees pose a serious threat because the IDs could be used to view sensitive network traffic or change, destroy, or steal critical data. When we brought these exceptions to the Department's attention, IT security staff continued to state that they were not being notified of employees' terminations in a timely manner. However based on documentation provided to us by Department staff we verified that of the 34 terminated users, the supervisors for 12 of the users had notified the IT security staff in a timely manner.

Further, specific to GenTax, we found that the Department has not documented standardized, written segregation-of-duties, profiles, or combination of profiles that are appropriate for different system users. Certain responsibilities should be segregated so that one individual does not control all critical stages of a process. Currently DOR does not have written segregation-of-duties rules, however some staff reported that duties are segregated within GenTax based on the user's job title. Our review of a sample of GenTax users raises questions about whether these informal rules are in fact in place. We found that users with the same job title had vastly different system privileges. In some cases the access privileges of staff with identical job titles varied by three levels (GenTax has 6 levels of review, with 0 having no review privileges and 5 having the most review privileges). We were subsequently informed that access to GenTax is determined by a supervisor and is not based on job titles. A written and well-defined policy would help the agency determine whether or not access granted to users is appropriate.

The Department should take immediate steps to correct the deficiencies we identified in the general computer controls over GenTax. First, the Department should immediately address the deficiencies we identified in the GenTax server configurations and provided to the Department under separate cover. Additionally, for future CITA phases, the Colorado Office of Cyber Security (OCS) should analyze the configuration and deployment of all critical servers prior to implementation and provide the Department with written notice of its conclusions and recommended changes. Second, the Department should require Fast Enterprises to 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. Finally, the Department should improve its

controls over user access to GenTax by immediately disabling all accounts belonging to terminated users; evaluating GenTax user profiles and identifying and documenting those profiles, or combination of profiles that are appropriate for different system users; ensuring that profiles or profile combinations that provide escalated system privileges are tightly controlled; and taking disciplinary action against all employees who fail to comply with established user access procedures.

(Classification of Finding: Significant Deficiency – See Appendix A)

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

Colorado Office of Cyber Security Response:

Agree. Implementation date: November 2009 for Phase 2 and prior to the implementation of subsequent phases.

The Office of Cyber Security (OCS) within the Governor's Office of Information Technology (OIT) will provide an in-depth assessment of CITA systems and their applications compared to the OCS hardening standards, the OCS Cyber Security Policies, and industry best practices. This will occur prior to the implementation of all future CITA phases. Upon completion of each effort, OCS will provide a prioritized and detailed remedial action plan to effectively manage all security weaknesses and vulnerabilities found during the assessment. Additionally, OCS will provide an annual vulnerability assessment of the CITA environment utilizing the OCS Threat & Vulnerability Management Program.

Department of Revenue Response:

Partially agree. Implementation date: June 2012.

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.

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.

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.

Department of Revenue Response:

a. Agree. Implementation date: June 2010.

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.

b. Agree. Implementation date: August 2009.

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.

c. Agree. Implementation date: October 2009.

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.

d. Agree. Implementation date: December 2009.

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.

e. Agree. Implementation date: December 2009.

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

Appendix A

Report Findings by Classification of Finding

Rec. No.	Page No.	Audit Finding	Classification of Findings		
			Material Weakness	Sig. Deficiency	Control Deficiency
1		Fix application-level control deficiencies in GenTax for future phases.			X
2		Improve controls over the data migration process for future phases.		X	
3		Periodically quantify risks to CITA and develop risk mitigation plans for the six high probability risks identified in our report.		X	
4 & 5		Address weaknesses in general computer controls.		X	

Definition of Finding Classifications	
Classification	Description
Material Weakness	A material weakness produces an immediate risk directly impacting the confidentiality, integrity, and availability of information systems and data. For IT projects, a material weakness represents an immediate threat to the overall success of the project. This would be considered a high risk finding.
Significant Deficiency	Significant deficiencies do not alone produce an immediate risk, but could affect the confidentiality, integrity, or availability of systems in conjunction with other factors. For IT projects, significant deficiencies do not represent an immediate threat to the overall success of the project but could result in project delays, cost overruns, or incomplete deliverables. This would be considered a moderate risk finding.
Control Deficiency	Control deficiencies do not present an immediate risk but could be indicative of operating deficiencies and/or have the potential to adversely affect the confidentiality, integrity, or availability of systems over an extended period of time. For IT projects, control deficiencies do not represent an immediate threat to the overall success of the project but could, over an extended period of time and in conjunction with other deficiencies, result in project delays, cost overruns, or incomplete deliverables. This would be considered a low risk finding.

The electronic version of this report is available on the website of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 2044