LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors:
James Gillett
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Kent Rice, Information Systems Audit Manager

CC: Dan Bucks, Director
Margaret Kauska, Administrator

DATE: September 2010

RE: IS Audit Follow-up (10DP-07): Integrated Revenue Information System Processing of Individual Income and Corporate Tax Records Department of Revenue (08DP-06)

INTRODUCTION

We presented our Information Systems audit of our review of processing of individual income and corporate tax records in the Integrated Revenue Information System (IRIS) to the Legislative Audit Committee in June 2009. The report contains three recommendations. The recommendations relate to:

- Identifying and removing access to terminated employees.
- Identifying unauthorized changes to programming code and tables.
- Implementing and testing a disaster recovery plan.

We requested and received information from Department of Revenue (DOR) personnel regarding progress toward implementation of our report recommendations. This memorandum summarizes their response and the audit work conducted to verify the response.

BACKGROUND

IRIS is a computer system implemented by DOR to maintain taxpayer records and process tax revenue. IRIS is a commercial-off-the-shelf system developed by a third-party vendor. In addition, IRIS has been customized to address the specific needs of the State of Montana. To date, the ability to process 38 of 39 tax types has been implemented, with only property tax being administered by a separate system.

IRIS is comprised of ten core modules, each providing different functions critical in tax administration. These modules are used by DOR users to maintain taxpayer records, process returns and payments, issue refunds, apply late penalties and interest rates, and identify and activate collection cases. In addition, IRIS is used as a tool to track tax audits, mail returns, and maintain tax-related transactions. Outside of the core functioning modules, DOR has developed modules specific to Montana, primarily to assist in customer relations, including a call center module used to track taxpayer calls and a fraud module, which retains returns suspected as fraudulent.

FOLLOW-UP DISCUSSION

The following sections summarize the report recommendations and progress towards implementing the recommendations.

Recommendation #1: We recommend the department implement controls to identify and remove access to terminated employees.

Implementation Status: Implemented

During our audit of IRIS, we identified nine individuals who no longer worked for DOR but still had active access to IRIS. In the past, DOR security relied on employee supervisors to provide notification when an employee left the agency. However, supervisors where not always providing notification and accounts were not being deactivated. In response, DOR developed a report to identify terminated employees so access can be removed. The report is designed to run every 89 days and identify all user accounts that have been inactive since the last report. The security officer reviews report results to determine if inactivity was due to termination. If so, the account will be deactivated. To confirm this, we reviewed the script behind the report and confirmed it is designed to extract users with 89 days of inactivity. Next we compared two reports to verify names that are identified as inactive are being removed. We verified DOR is identifying and removing inactive users.

Recommendation #2: We recommend the department actively review changes to production code and database tables for authorization.

Implementation Status: Implemented

Another finding in our audit of IRIS identified two developers who had uncontrolled access to production code and databases giving them the ability to modify database and programming code without approval or oversight. To track and monitor changes to the production code and database tables, DOR has implemented two software tracking packages that allow staff to actively review changes to production code for authorization. One of the software packages holds all code being migrated from the test environment to production. Only one DOR manager has access to the repository and uses this tool to review migrated changes and if acceptable, move them on to production. This not only allows for review of the changes, but also requires DOR staff to approve changes.

The other new software addition is a tool that logs all changes to the database structure. This allows DOR staff the ability to review database changes prior to implementation. In addition, the software will not release the changes for implementation without approval from DOR staff.

Recommendation #3: We recommend the department develop, implement, and test a documented plan to recover the Integrated Revenue Information System in the event of a disaster or major outage.

Implementation Status: Implemented

During our audit of IRIS, we found DOR had not implemented and tested a disaster recovery plan to recover IRIS in the event of a significant outage of the system. In February 2010, we performed a separate audit on disaster recovery planning efforts statewide, with an overall recommendation to the Department of Administration (DOA) to establish criteria when developing a disaster recovery plan. During the audit, we met with DOR staff to determine its disaster recovery status. At that time, they had developed a Continuity of Operations Plan (COOP) that included disaster recovery elements. Currently, the COOP is still in place and testing protocols to recover IRIS have been developed in the form of recovery protocols to prepare for the migration of hardware to the new State datacenter. Following the migration of IRIS hardware to the new datacenter, we confirmed the existence of testing methodology and verified a successful recovery.