



A REPORT
TO THE
MONTANA
LEGISLATURE

INFORMATION SYSTEMS AUDIT

*Integrated Revenue
Information System:
Processing of Individual
Income and Corporate Tax
Records*

Department of Revenue

MAY 2009

LEGISLATIVE AUDIT
DIVISION

08DP-06

**LEGISLATIVE AUDIT
COMMITTEE**

REPRESENTATIVES

DEE BROWN
BETSY HANDS
SCOTT MENDENHALL
CAROLYN PEASE-LOPEZ
WAYNE STAHL
BILL WILSON

SENATORS

GREG BARKUS
JOHN BRENDEN
TAYLOR BROWN
MIKE COONEY
CLIFF LARSEN
MITCH TROPILA

AUDIT STAFF

INFORMATION SYSTEMS

STEPHEN R. DAEM
DEON R. OLSON
KENT RICE
DALE STOUT
NATHAN TOBIN

FRAUD HOTLINE
HELP ELIMINATE FRAUD,
WASTE, AND ABUSE IN
STATE GOVERNMENT.

CALL THE FRAUD
HOTLINE AT:

(STATEWIDE)
1-800-222-4446
(IN HELENA)
444-4446

INFORMATION SYSTEMS AUDITS

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit 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 finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

Reports can be found in electronic format at:

[Http://leg.mt.gov/audit](http://leg.mt.gov/audit)

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel



Deputy Legislative Auditors
James Gillett
Angie Grove

May 2009

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of the Integrated Revenue Information System (IRIS). The Department of Revenue (DOR) operates and maintains IRIS to assist in the administration of taxpayer records and transactions. The focus of the audit was to determine that IRIS was operating as expected in its functions of maintaining customer records, processing individual and corporate tax returns, and processing payments made by taxpayers. Additionally, this audit addressed security controls in place to maintain the integrity of IRIS and tax data.

Overall, we found DOR has controls in place to ensure IRIS is accurately processing individual income and corporate tax submissions, as well as securing the IRIS system. However, we identified areas where DOR can improve. As a result, we have issued three recommendations relating to identifying and removing access to terminated employees, identifying unauthorized changes to programming code and tables, and improving business continuity of IRIS operations by implementing and testing a disaster recovery plan.

We wish to express our appreciation to the Department of Revenue for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

TABLE OF CONTENTS

| | |
|--|------------|
| Figures and Tables..... | ii |
| Appointed and Administrative Officials | iii |
| Report Summary | S-1 |
| CHAPTER I – INTRODUCTION AND BACKGROUND | 1 |
| Introduction..... | 1 |
| Audit Objectives..... | 2 |
| Audit Scope and Methodology | 2 |
| Audit Overview..... | 3 |
| CHAPTER II – PROCESSING OF INCOME AND CORPORATE TAXES | 5 |
| Introduction..... | 5 |
| IRIS Based on a Commercially Produced System..... | 5 |
| Scenario Testing and Change Management Confirm IRIS is Meeting Department Needs..... | 6 |
| IRIS Will not Process Records with Missing Data | 7 |
| Tax Rates in IRIS are Accurate | 7 |
| CHAPTER III – IRIS SECURITY | 9 |
| Introduction..... | 9 |
| ITSD is Securing IRIS Hardware | 9 |
| DOR is Securing IRIS Desktops | 10 |
| DOR has Limited Access to IRIS through Policy of Least Privilege..... | 10 |
| Terminated Employees with Active IRIS Accounts | 11 |
| DOR Needs to Strengthen Controls over Access to Production Code and Data..... | 12 |
| CHAPTER IV – DISASTER RECOVERY | 13 |
| Introduction..... | 13 |
| DOR has not Implemented a Disaster Recovery Plan..... | 14 |
| DEPARTMENT RESPONSE | A-1 |
| Department of Revenue | A-3 |

FIGURES AND TABLES

Figures

| | | |
|----------|---|----|
| Figure 1 | Core Processing Modules of IRIS | 1 |
| Figure 2 | States, Locals, and Provinces Using Gentax..... | 6 |
| Figure 3 | Security Responsibilities of IRIS Components..... | 9 |
| Figure 4 | Scenarios Identified in Nationwide Survey of IT Managers..... | 13 |

APPOINTED AND ADMINISTRATIVE OFFICIALS

Department of Revenue

Dan Bucks, Director

Margaret Kauska, Administrator, Information Technology and Processing
Division

Larry Logan, Chief, Information Technology Bureau

Gene Walborn, Administrator, Business and Income Taxes Division

Steve Austin, Administrator, Citizens Services and Resource Management
Division

Cleo Anderson, Chief Security Officer

REPORT SUMMARY

Department of Revenue – Integrated Revenue Information System

The Integrated Revenue Information System (IRIS) is a computer system implemented by the Department of Revenue (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. The final component, allowing for online e-filing through IRIS, is scheduled to be completed by June 2009.

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.

All IRIS components and functionality within IRIS play important roles in the tax administration process; however, IRIS consists of multiple modules and tax types. Because of the complexity and size of the system, we limited audit scope. Through our assessment of audit risk we identified creation and maintenance of taxpayer records, input of tax returns and payments, and processing of transactions as key elements of the IRIS system. As a result, our audit work focused on those functions, which include the Customer, Returns, Payments, and Transaction modules of IRIS. In addition, we limited our audit work to tax data and processing associated with individual income and corporate tax, which on an annual basis produce the majority of tax returns and revenue for the department.

This report discusses the work performed during this audit, including findings and recommendations. Overall, we conclude DOR has controls in place to ensure IRIS is accurately processing individual income and corporate tax submissions, as well as adequately securing the IRIS application. However, we did identify areas where DOR can improve. This report includes three recommendations for DOR to identify inappropriate and unauthorized changes to programming code and database tables, identify and remove access from terminated employees, and implement and test a disaster recovery plan.

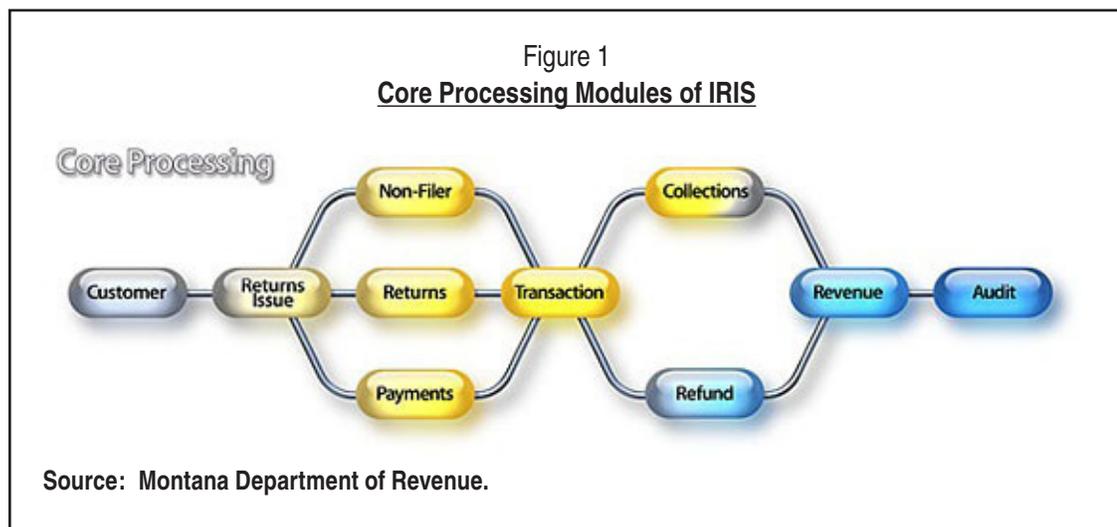
Chapter I – Introduction and Background

Introduction

In December 1999, the Department of Revenue (DOR) implemented the first phase of the Process Oriented Integrated System (POINTS), a computer application designed to integrate the administration of all tax types and taxpayer accounts under one umbrella system. To best meet the needs of the State of Montana and DOR, POINTS was conceived as a custom system to be developed in-house by DOR developers with the assistance of a third-party vendor. Because of processing and data integrity issues, legislation was passed in Chapter 597, Laws of 2003 (15-1-140, MCA) requiring the replacement of POINTS with a new integrated tax administration system.

In 2004, DOR began phasing in the replacement system, the Integrated Revenue Information System (IRIS). The core of IRIS is a commercial-off-the-shelf (COTS) system developed by a third-party vendor. IRIS also can be customized to accommodate the specific needs of the State of Montana, as well as reflect requirements and thresholds detailed in statute. To date, the ability to process 38 of 39 state tax types has been implemented, with only property tax being administered in a separate system. An online component, allowing for online e-filing through IRIS, is scheduled to be completed by June 2009.

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. The following figure illustrates the module structure of IRIS.



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.

IRIS also serves to export and receive data from external systems. In particular, the majority of individual and corporate returns are not entered directly in IRIS; rather, they are created using third-party tax preparation software applications (i.e. TurboTax, H&R Block). IRIS is designed to accept and upload returns from a third-party through a periodic batch process. This allows Montana's taxpayers to e-file their state tax returns simultaneously with their federal returns. Also, IRIS interfaces with the Statewide Accounting, Budgeting, and Human Resources System (SABHRS) to upload current account activity, including revenue received and refunds remitted. In the event refunds are remitted, IRIS also interfaces with the warrant writing function in SABHRS to issue payment to taxpayers.

Audit Objectives

Considering the role IRIS plays in the maintenance of taxpayer records and the processing of tax revenue for state government, it is imperative the system is accurately processing and calculating tax-related transactions and maintaining the integrity of taxpayer data records. Due to the critical elements of the system, and the reliance both state government and Montana taxpayers place on IRIS, we conducted audit work to address the following objectives:

- ◆ Determine if IRIS taxpayer and return information is complete and accurate.
- ◆ Determine if IRIS taxpayer returns and account balances are calculated completely and accurately.
- ◆ Determine if access controls are in place to prevent inappropriate or unauthorized access to IRIS.
- ◆ Determine if security and business continuity controls are in place to maintain continued operation of IRIS.

Audit Scope and Methodology

Although all components and functionality within IRIS play important roles in the tax administration process, because IRIS consists of multiple modules and serves 38 different tax types, we limited audit scope. Through our assessment of risk, we identified creation and maintenance of taxpayer records, input of tax returns and payments, and processing of transactions as key elements of the IRIS system. As a result, our audit work focused on those functions, which involve the Customer, Returns, Payments,

and Transaction modules of IRIS. In addition, we limited audit work to tax data and processing associated with individual income and corporate tax, which on an annual basis produce the majority of tax returns and revenue for the department.

Even if IRIS functionality is working as expected, outside influences can still affect system operations and integrity. Consequently, we included the security of the IRIS application and hardware in the scope of this audit. We also looked at DOR's plans to ensure continued operations of the system in the event of a disaster or major outage.

Testing of IRIS functionality and controls was conducted through a combination of staff interviews, review of agency documentation, observation of IRIS processes, and extraction and analysis of IRIS data using a computer-assisted audit tool.

This audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office (GAO). We evaluated the control environment using state law and generally applicable and accepted information technology standards established by the IT Governance Institute.

Audit Overview

Based on our work, we conclude DOR has controls in place to ensure IRIS is accurately processing individual income and corporate tax submissions, as well as adequately securing the IRIS application. However, we did identify areas where DOR can improve, specifically in identifying inappropriate and unauthorized changes to programming code and database tables, as well as improving the continuity of IRIS operations by implementing and testing a disaster recovery plan. The remainder of this report discusses our findings and recommendations.

Chapter II – Processing of Income and Corporate Taxes

Introduction

In order to rely on system processes, we have to verify the accuracy of internal calculations and data entry. In terms of processing, we identified two factors which assured us we can rely on the Integrated Revenue Information System (IRIS) to accurately process income and corporate taxpayer accounts and returns. These factors include the delivered processing of a commercial-off-the-shelf (COTS) system and the extensive scenario and system testing performed by the Department of Revenue (DOR). Once we were assured the system was processing effectively, we wanted to confirm the integrity of the data processed. This included verifying system controls are in place to require complete entry of all required data. Additional testing involved confirming tax and penalty rates in IRIS are accurate based on statute. The remainder of this chapter discusses the work we conducted in these areas and our findings.

IRIS Based on a Commercially Produced System

The core of IRIS is a COTS system called Gentax, which is a tax processing application currently in use by tax revenue agencies in 14 different states and three provinces. One of the benefits of implementing a COTS system is assurance the application is working as the developer intended. This is confirmed by the testing process performed by the vendor prior to release of the product. Once the product is released, the successful implementation and use by other entities demonstrates the product can be relied on. The following figure details all states, provinces, and local municipalities that have successfully integrated Gentax as the primary tax revenue administration system.

Figure 2
States, Locals, and Provinces Using Gentax



Source: Compiled from vendor documentation.

Scenario Testing and Change Management Confirm IRIS is Meeting Department Needs

Although IRIS may be working as the developers intended, this does not mean the system is meeting the requirements of DOR and the State. To ensure IRIS functionality is working as expected and providing the necessary functionality to process tax revenue for the State, DOR has performed testing of IRIS. Department testing included developing numerous scenarios to run on IRIS to ensure the system can handle all possible hypothetical instances that may arise. During our audit, we verified DOR had tested IRIS prior to implementation. As a result, we can confirm the agency has an understanding of the functionality provided by IRIS and have concluded the system meets its requirements.

In instances where the baseline processing of IRIS does not meet the needs of DOR, enhancements can be made to provide more customized functionality. DOR has made a number of enhancements to IRIS, which have not gone through the same vendor testing process as the baseline system. One example includes the development of an enhancement responsible for calculating interest on an outstanding tax balance. To ensure this calculation, and other enhancements, are working properly, DOR has developed a change management process to ensure all changes to the system are requested by management and tested to verify proper functioning prior to migration to the production version of IRIS. DOR testing documentation verifies the agency follows this process for all enhancements, and as a result, can rely on those enhancements to work as expected.

IRIS Will not Process Records with Missing Data

Although the internal processing of IRIS may be functioning properly, inaccuracies can still occur if tax data is not entered properly or is missing altogether. When new taxpayer accounts or tax returns are entered, it is necessary for certain information to be present in order for IRIS to process the records. For example, when a new taxpayer record is entered, a name and address are required. When a new tax return is entered, the tax type and filing period are two pieces of information required by IRIS to process the return.

Audit work was conducted to ensure necessary data is entered in IRIS every time new taxpayer accounts and returns are created. IRIS has edits in place forcing the user creating the new records to enter all required information. Edits are components of a system that notify a user when a required field of data has not been entered and will not allow the record to be saved until all required fields are entered. We worked with DOR personnel to identify all necessary fields for a complete taxpayer account and submitted tax return. Through query of IRIS, we were able to confirm all required fields were complete for all existing taxpayer and return records.

Tax Rates in IRIS are Accurate

The tax rates for individual and corporate tax are established by state statute, meaning they are specific to Montana and are subject to change. As a result, DOR is responsible for ensuring the tax and interest rates in IRIS are current and accurate. If these rates are not accurate in IRIS, then calculation of tax liability and interest penalties will be incorrect. To verify the accuracy of tax rates in IRIS, we compared the rates found in IRIS with the following rates established in statute:

- ◆ Tax rate for individuals (15-30-103, MCA)
- ◆ Tax rate for corporations (15-31-121, MCA)

- ◆ Penalty rate for individuals (15-1-216, MCA)
- ◆ Penalty rate for corporations (15-1-216, MCA)

Based on our testing, all individual and corporate tax rates and penalty rates in IRIS are accurate.

CONCLUSION

Considering the testing processes implemented by the vendor and Department of Revenue, as well as the requirements for complete data, and existence of accurate rates, we conclude IRIS can be relied on to accurately process and calculate taxpayer and return records for individual and corporate tax types.

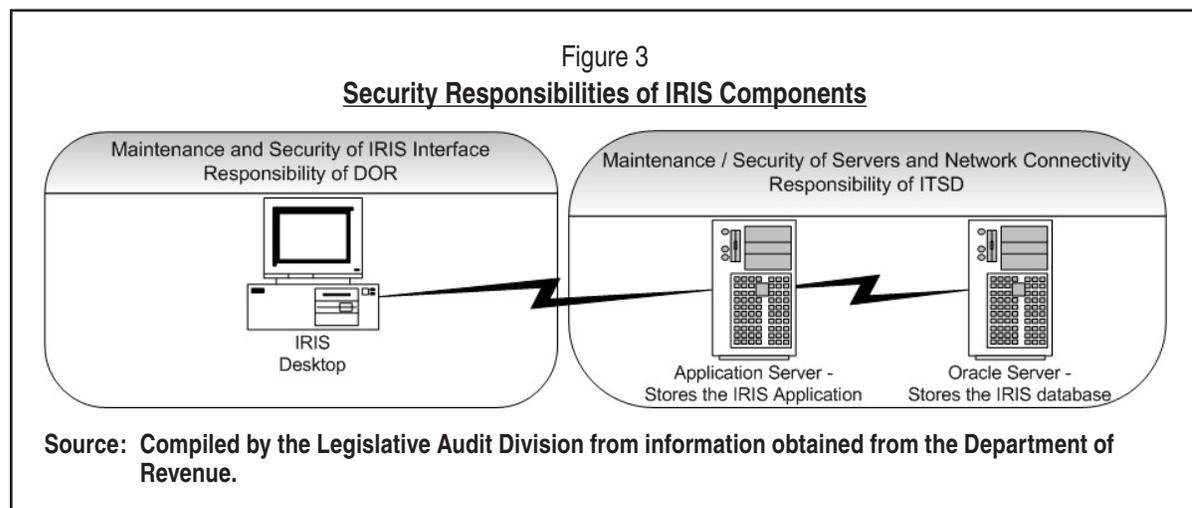
Chapter III – IRIS Security

Introduction

Through audit work, we were able to confirm critical Integrated Revenue Information System (IRIS) processes are working as expected. However, without strong security controls, IRIS processing can be exploited or damaged. During this audit, we conducted work to ensure the Department of Revenue (DOR) has taken measures to secure hardware where the IRIS application and data are stored and computer desktops used to access IRIS. We also performed work to ensure access granted to the over 400 users is appropriate and authorized by management. Overall, we found IRIS hardware is adequately secure. We also verified DOR has implemented a management review process to ensure access is limited to only appropriate users at a level approved by management. However, we also identified risk associated with a limited number of user accounts. This chapter discusses the work performed in the area of IRIS security and details our findings.

ITSD is Securing IRIS Hardware

DOR has contracted with the Information Technology Services Division (ITSD), Department of Administration, to host and maintain the servers where the IRIS application and databases reside. Figure 3 illustrates how maintenance and security responsibilities of IRIS are dispersed.



One of the services provided by ITSD is to update the servers with the most current security patches and updates to protect them from external threats resulting from vulnerabilities. During a previous Information Systems audit (08DP-02), we reviewed ITSD's process for updating and maintaining servers. Based on that audit work, we can rely on ITSD processes to ensure IRIS servers are current with the latest security updates and patches.

DOR is Securing IRIS Desktops

All computers at the DOR are installed with IRIS. Consequently, each of these desktops acts as an access point to IRIS, and if not properly secured could be used to access and exploit IRIS data through a computer virus or by an external hacker. As with the servers, DOR can limit this risk by ensuring all desktops are installed with the latest security patches and anti-virus definitions. During our audit, we performed testing to verify this.

We compared DOR's inventory of all desktops with the list of all desktops recently patched and updated with the latest anti-virus definition. Audit work found controls in place to automatically update desktops with current patches and anti-virus when they are connected to the state network. Our comparison found this process to be working as all desktops connected to the network were current. The remaining desktops were not current, but since they were not connected to the network, there was no risk of being infected. In addition, as soon as these desktops are connected to the network, they will be automatically updated.

CONCLUSION

Between ITSD and Department of Revenue maintenance of IRIS servers and desktop computers, we conclude security controls are in place to protect hardware from external threats.

DOR has Limited Access to IRIS through Policy of Least Privilege

IRIS contains records for 1,193,039 taxpayers, including personal data and state and federal tax information. The Department of Revenue is charged with the maintenance and protection of this data, and both federal and state law requires DOR and individual IRIS users to maintain confidentiality. We performed audit work to ensure DOR is securing IRIS data from internal threats. A primary means of protecting confidential and sensitive data from internal threats is to limit access to it; specifically, limiting the ability to view, create, modify, or delete records. Currently, DOR has granted access to IRIS to over 400 users to perform various activities.

To limit the number of users who have access to IRIS data, and to limit those with access to only modules and abilities in line with their job duties, DOR has implemented a policy of 'least privilege' where access is granted based on the job requirements of the user. To enforce this policy, DOR has implemented a management review process

where all access requests require duplicate levels of approval from the DOR security officer and the Director's Office. During the course of the audit, we were able to verify this process has been implemented and executed by DOR and confirmed all user access granted to IRIS aligns with DOR policy.

Terminated Employees with Active IRIS Accounts

Although DOR has effectively implemented a process to limit access to IRIS, improvements can be made in managing existing user accounts. Specifically, we identified nine individuals who no longer work for DOR, but still had active access to IRIS. Typically, there is a risk that former employees could use active accounts to obtain access to sensitive and confidential information which they are no longer authorized to see. This scenario is unlikely given these nine users no longer have access to the State's network, which is required to access the IRIS system. However small the risk, best practices suggest a terminated employee's access should expediently be deactivated in order to remove any and all risk.

We notified DOR of the terminated users with active accounts. They have since taken steps to remove the accounts. They have also implemented a new process to better identify terminated employees and deactivate their access. In the past, the DOR security officer relied on supervisors throughout the agency to provide notification when an employee left the agency. However, we found supervisors were not always notifying the security officer and the accounts were never deactivated.

To resolve this issue, DOR has implemented a process to identify all employees who have not used their IRIS access for a certain period of time. The security officer will then contact the employees' supervisors and verify if the access is still required. If the access is no longer needed, or the employee no longer works for DOR, the account will be deactivated. We have not verified the effectiveness of the new control.

RECOMMENDATION #1

We recommend the Department of Revenue implement controls to identify and remove access to terminated employees.

DOR Needs to Strengthen Controls over Access to Production Code and Data

Another area where DOR can improve when granting access is to limit the ability of IRIS developers to make changes directly to programming code and database data, thus bypassing change control procedures. Best practices require segregation of duties. Developers should make changes to the system in a test environment, and then a DOR employee should migrate the changes to the production environment. This limits the risk of knowledgeable and able individuals from altering and manipulating programming code and data.

Audit work identified two developers with full administrative access to IRIS, giving them the ability to modify both the IRIS database and programming code without oversight or approval. DOR recognizes this is not the ideal scenario, but claims there are not enough qualified staff to segregate duties between development and migration of code and data. As a result, they have to overlap duties with some of their more knowledgeable staff; however, without segregation of duties, there should be some type of compensating control. DOR has the ability to monitor changes to IRIS and management could review all updates to production code and data to determine if the changes have been authorized. The department is currently in the process of developing a solution.

RECOMMENDATION #2

We recommend the Department of Revenue actively review changes to production code and database tables for authorization.

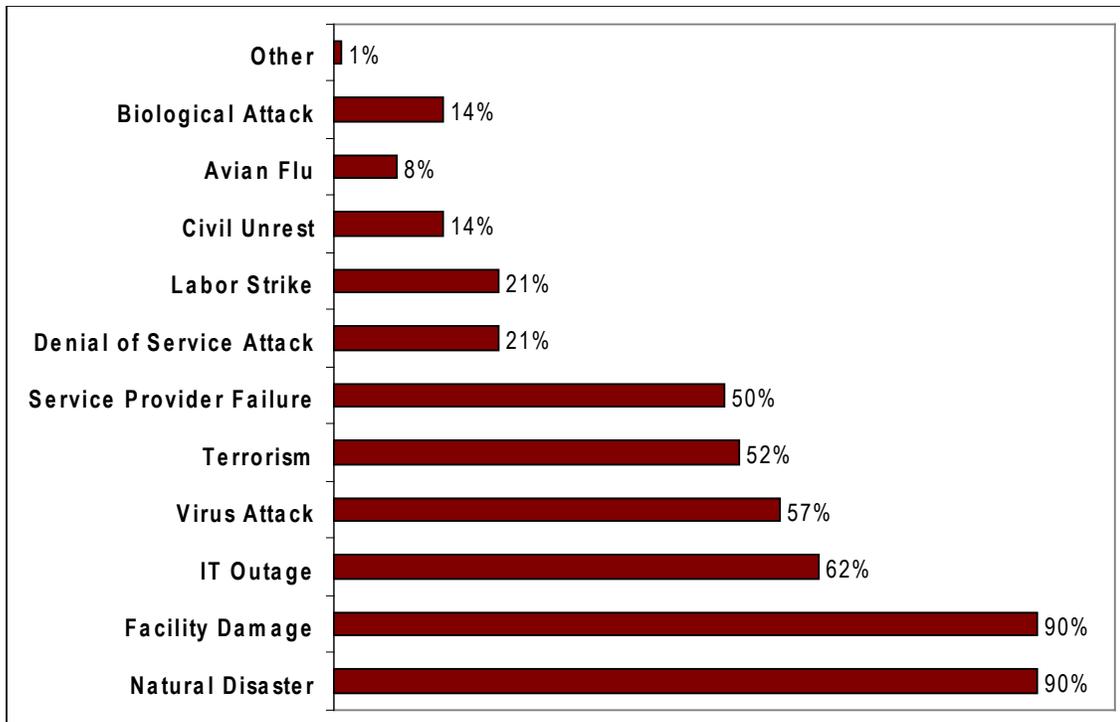
Chapter IV – Disaster Recovery

Introduction

An important responsibility of the Department of Revenue (DOR) is to maintain the availability of the Integrated Revenue Information System (IRIS) in the event of a disaster or major outage. IRIS is critical to processing taxpayer records and tax returns, and any long term outage of the system may result in a loss of state revenue and an overall inconvenience to both the State and taxpayers.

There are a number of events that could occur, resulting in a loss of IRIS operations. The worse case scenario would involve a natural disaster. Although not entirely likely, Helena does have a history of strong seismic activity and has been the victim of earthquakes in the past. While not as significant, other events such as flooding, theft, electrical outages, fire, and human error can damage critical IRIS components, potentially resulting in the inability to process revenue for the state. Figure 4 below lists scenarios identified by 222 Information Technology managers nationwide as potential disasters.

Figure 4
Scenarios Identified in Nationwide Survey of IT Managers



Source: Gartner.com, IT Research and Advising Company.

DOR has not Implemented a Disaster Recovery Plan

To mitigate the damage resulting from major and minor disasters, best practices require organizations to implement a disaster recovery plan. In other words, the organization should develop policies, plans, and procedures to regain access to data, workspace, lines of communication, and critical business processes. During our audit work, we noted DOR has not developed a disaster recovery plan to recover IRIS in the event of a disaster or major outage. As a result, DOR has not established details on how IRIS will be recovered. In addition, DOR cannot provide an estimated time frame as to when IRIS would be operational and processing tax revenue.

DOR management is aware of the need for a disaster recovery plan and consider it a critical aspect of operations. While management recognizes the importance of having a disaster recovery plan, they state developing and testing would require financial and staffing resources they cannot afford to devote at this time. DOR management believes an entire full-time position would be required to develop, test, and maintain an effective disaster recovery plan. As this point, they are not prepared to move an existing employee into the position as it may take away from the revenue collection process.

Although there can be significant costs associated with developing and testing a disaster recovery plan, the cost of attempting to recover missing data, purchasing new hardware and other unplanned operations will be far more excessive. While we cannot provide specifics on the cost of not having a disaster recovery plan, a study by a leading disaster recovery organization, Kings Bridge, shows 70 percent of all organizations affected by a major disaster will never recover because they did not establish a plan to recover their business processes, including Information Technology systems. Given the mission of DOR, the department is not at risk of never recovering; however, there will be additional costs and loss of revenue when attempting to recover downed and damaged operations without a solid plan.

RECOMMENDATION #3

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

DEPARTMENT OF
REVENUE

DEPARTMENT RESPONSE



Dan Bucks
Director

Montana Department of Revenue



A-3

Brian Schweitzer
Governor

April 24, 2009

Tori Hunthausen, Legislative Auditor
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena, MT 59620-1705

RECEIVED

APR 24 2009

LEGISLATIVE AUDIT DIV.

Dear Ms. Hunthausen:

Thank you for the opportunity to respond to recommendations presented in the April 2009 Information Systems Audit Report entitled Integrated Revenue Information System: Processing of Individual and Corporate Tax Records. Our response to those recommendations is as follows:

Recommendation #1

We recommend the Department of Revenue implement controls to identify and remove access to terminated employees.

Concur. The Department of Revenue (DOR) Information Security Officer now produces and reviews a monthly report identifying the Integrated Revenue Information System (IRIS) user accounts that have been inactive over 89 days. In addition, DOR has, in conjunction with the Department of Administration (DOA) Information Technology Services Division (ITSD), implemented a monthly review of Active Directory accounts. This review ensures that both user IDs and workstation IDs are removed from the Active Directory when dormant in excess of 89 days. These new measures, coupled with the existing procedures and processes to limit IRIS access, will better ensure that only authorized users have active accounts.

Recommendation #2

We recommend the Department of Revenue actively review changes to production code and database tables for authorization.

Concur. From system implementation, DOR Information Technology (IT) has had access to IRIS migration logs to provide an audit trail of programming and configuration changes made to the system. We have used this tool to confirm the migration of production code but have not used it to specifically identify unauthorized changes. DOR IT is developing a dual-control process, assigning two DOR employees the responsibility of reviewing the IRIS system migration logs. DOR employees will verify that the migration was authorized and ensure the appropriateness of programming and configuration changes made to DOR site specific code.

It must be noted, however, that the best practices referred to in the audit report assume a traditional agency/vendor relationship with the agency taking ownership of the software through a licensing agreement.

Dan Bucks
Page 2
4/24/2009

IRIS was developed using the Commercial-Off-The-Shelf (COTS) product GenTax which was built by Fast Enterprises. As a COTS product, DOR does not own the IRIS core code. Consequently, while DOR IT employees will verify who initiated the migration of core code changes and the authorization of such, they will not be able to review the code itself for appropriateness. As long as the department uses the GenTax product, the vendor will, to some degree, have a presence in DOR's production environment.

At this time, the GenTax product is used in 21 different tax jurisdictions. The product is proven, as are the best practices utilized by FAST Enterprises in its implementation and support. It is in their best interest to do nothing to jeopardize the trust relationship they have with DOR.

Recommendation #3

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

Concur. DOR fully understands the need to develop, implement, and test a documented plan to recover not only IRIS but all DOR systems. However, DOR has previously been unable to allocate existing resources to this effort. The department did identify disaster recovery as a high priority for the 2008-2009 biennium by including it in our IT strategic plan and requested funding and FTE to put an adequate disaster recovery program in place. This request was unfortunately denied by the 2007 Legislature.

Despite the lack of a documented disaster recovery plan, DOR has in place Continuity Of Operations Plans (COOP). Within the COOP are procedures and a list of business processes and services that will drive the restoration prioritization of IT applications and systems should a disaster or emergency occur. The severity, extent and type of disaster or emergency will determine the restoration plan implemented and subsequently the system recovery prioritization.

Additionally, DOR will soon be a part of the redundancy and failover capabilities of the new data centers in Helena and Miles City as well as the tape/backup facility in the Helena Federal Reserve Building. DOR will rely on these ITSD facilities for disaster recovery services for its critical systems such as IRIS. As these facilities become available, DOR will test the redundancy/failover services with ITSD to ensure service level agreements match system recovery time objectives.

Thank you for allowing us the opportunity to review and respond to the audit report and your recommendations. We appreciate the open discussion we had with you, Kent Rice, Dale Stout and Nathan Tobin and would like to thank all who participated in the audit for their professionalism and their willingness to work with the department.

Sincerely,



Dan Bucks, Director
PO Box 5805
Helena, MT 59604-5805