Secretary of State
Oregon Audits Division

Department of Revenue

Recommendation Follow-up Report: DOR Has Improved its GenTax System Controls, but Disaster Recovery Weaknesses Remain

June 2019
2019-25

Secretary of State Bev Clarno
Audits Division Director Kip Memmott

Follow-up to Audit Report 2018-08

Department of Revenue

Recommendation Follow-up Report: DOR Has Improved its GenTax System Controls, but Disaster Recovery Weaknesses Remain

June 2019

Follow-up Summary

The Oregon Department of Revenue (DOR) made steady progress on nine of the 11 recommendations from the original audit, fully implementing four. However, work remains to further refine some changes the agency made to improve its processes for logical access. In addition, significant risks posed by a lack of disaster recovery planning remain.

Findings from the Original Audit

- DOR's GenTax system generally has sufficient controls to ensure accuracy in processing tax data.
- Logical access and change management controls, while generally sufficient, need improvement.
- There is a risk GenTax will not be timely restored in the event of a disaster or major disruption.
- DOR did not obtain independent verification the GenTax vendor implemented appropriate controls to ensure the security of Oregon data.

Improvements Noted

- The agency has improved its procedures to ensure missing interface files are tracked and reviewed. (pg. 2)
- Management made progress in improving procedures for logical access controls. (pgs. 2-3)
- Some technical solutions have been introduced that not only address our recommendations, but go one step beyond simply developing new procedures. (pg. 5)

Remaining Areas of Concern

- The agency has not finalized or tested disaster recovery plans. (pg. 4)
- DOR has declined to pursue our recommendation to obtain an independent assessment of vendor security controls at this time. (pg. 4)

Introduction

The purpose of this report is to follow up on the recommendations we made to the Oregon Department of Revenue (DOR) as included in audit report 2018-18, "GenTax Accurately Processes Tax Returns and Payments, but Logical Access and Disaster Recovery Procedures Need Improvement."

The Oregon Audits Division conducts follow-up procedures for each of our performance audits. This process helps assess the impact of our audit work, promotes accountability and transparency within state government, and ensures audit recommendations are implemented and related risks mitigated to the greatest extent possible.

We use a standard set of procedures for these engagements that includes gathering evidence and assessing the efforts of the auditee to implement our recommendations; concluding and reporting on those efforts; and employing a rigorous quality assurance process to ensure our conclusions are accurate. We determine implementation status based on an assessment of evidence rather than self-reported information. This follow-up is not an audit, but a status check on the agency's actions.

To ensure the timeliness of this effort, the division asks all auditees to provide a timeframe for implementing the recommendations in our audit reports. We use this timeframe to schedule and execute our follow-up procedures.

Our follow-up procedures evaluate the status of each recommendation and assign it one of the following categories:

- **Implemented/Resolved**: The auditee has fully implemented the recommendation or otherwise taken the appropriate action to resolve the issue identified by the audit.
- **Partially implemented**: The auditee has begun taking action on the recommendation, but has not fully implemented it. In some cases, this simply means the auditee needs more time to fully implement the recommendation. However, it may also mean the auditee believes it has taken sufficient action to address the issue and does not plan to pursue further action on that recommendation.
- **Not implemented**: The auditee has taken no action on the recommendation. This could mean the auditee still plans to implement the recommendation and simply has not yet taken action; it could also mean the auditee has declined to take the action identified by the recommendation and may pursue other action, or the auditee disagreed with the initial recommendation.

The status of each recommendation and full results of our follow-up work are detailed in the following pages.

We sincerely appreciate the courtesies and cooperation extended by officials and employees of DOR during the course of this follow-up work.

Recommendation Implementation Status

Recommendation #1

Consider notifying taxpayers claiming no withholding if withholding records are found.	**Implemented/ Resolved**

Our original audit found 0.2% of Form 40 tax returns where the taxpayer claimed no withholding, but W-2 and 1099 records employers submitted showed withholding for the taxpayer. DOR leadership agreed with the recommendation and considered the risks and impact of changing their notification processes. They determined the risk to be low and chose not to take additional action. Because DOR appropriately considered the risk, we concluded this recommendation is resolved.

Recommendation #2

Implement controls to track and analyze how interface file failures are resolved.	**Implemented/ Resolved**

The original audit found DOR was monitoring interface file failures between other systems and GenTax, but was not documenting resolution of missing interface files. DOR updated their procedures to track and evaluate interface file failures by documenting reasons for the missed files and identifying any further steps or expectations for resolution. We tested a selection of daily interface reports and identified missing files. We reviewed the notes for these files and determined the updated procedures were being appropriately followed.

Recommendation #3

Identify and document which GenTax roles should not be combined with others.	**Implemented/ Resolved**

DOR identified the roles in GenTax that should not be combined to prevent users from having potentially conflicting duties and documented the reasoning, which was sufficient to implement the recommendation.

The agency took further action by identifying users currently having these conflicting combinations of roles. DOR managers also recognized there may be some situations where individuals need the conflicting access to perform valid business functions. For these users, DOR is developing a report that will identify whether any of these individuals used the conflicting access inappropriately. For example, there is a higher risk of improper payments when a user can both create a customer in GenTax and process a refund to that customer. This report would assist management in identifying when both actions were taken for the same customer. In addition to the creation of the report, work remains to remove the conflicting access from users without a business need.

Recommendation #4

Fully document GenTax groups and functions and ensure managers have received instructions on how to request access.	**Partially implemented**

DOR updated training materials for managers to provide instructions on how to view GenTax groups and functions, and how to request access for their employees, including providing examples of acceptable and unacceptable language to use in making the request.

However, DOR has not yet conducted this training for most managers, and the identification of GenTax roles from recommendation no. 3 has not been integrated into the documentation used for requesting access. This integration is needed to ensure managers do not mistakenly ask for potentially conflicting roles.

Recommendation #5

Improve procedures to ensure user access is removed timely and completely when no longer needed.	**Partially implemented**

This recommendation applied to two specific areas of weakness. First, users who had terminated employment with DOR did not always have their access removed timely. Second, users who transferred positions within DOR did not always have their new access permissions updated to remove access that was no longer needed.

During the audit, DOR had a procedure that instructed managers to request removal of access for terminated or transferred employees. Our testing showed this administrative control did not always function appropriately. DOR also had implemented a compensating control during the audit — a monthly comparison of terminated employees to a list of access requests to ensure managers had requested access be terminated — though procedures for this control had not been formalized at the time.

DOR has since developed a draft procedure for requesting access removal for transferred employees. The procedure improves the prior practice by specifying that previous access will be removed upon request for new access, though this is still dependent upon the new manager requesting access. However, the agency has not yet formalized these changes. In addition, DOR has not yet documented the methodology it uses for the monthly review of terminated employees.

Recommendation #6

Update policy to require periodic manager review of logical access granted to GenTax and develop a mechanism to enforce and document the review.	**Partially implemented**

DOR has developed draft language to update policies and procedures so that periodic manager review of access is required, but it has not yet formally approved the changes. The agency is also developing an automated solution for conducting and documenting manager reviews. This action should help ensure periodic review is performed and documented, but this effort is not yet complete.

Recommendation #7

Implement monitoring of logs to identify inappropriate activity taken by server administrators.	**Implemented/ Resolved**

DOR implemented tools and developed reports to monitor certain types of potentially anomalous actions that may be taken by server administrators and others. Several of these reports and tools existed during the audit, but the reports now include additional servers. While there are still opportunities to expand monitoring into more detailed activities, we concluded DOR has implemented appropriate compensating controls based on their current set of monitoring tools.

Recommendation #8

Develop more specific guidance for individuals testing system changes to ensure that all elements are appropriately considered.	**Partially implemented**

DOR improved guidance associated with documenting test plans and identifying what test information is expected to be documented. However, more work is needed to further define the specific elements to be included in test plans.

Recommendation #9

Develop and maintain a written disaster recovery plan for GenTax.	**Partially implemented**

Since the audit was completed, DOR developed a disaster recovery plan that addressed GenTax recovery at a theoretical level. However, the proposed tactical recovery techniques had not been completed, tested, or verified by DOR. In addition, since this plan was completed, the disaster recovery approach for GenTax has shifted. DOR is now pursuing an alternate recovery strategy that is in the planning stages and requires approval from the Internal Revenue Service due to the type of data involved. We concluded that while progress is being made, much more work remains to implement this recommendation.

Recommendation #10

Periodically test backups stored offsite to ensure they can be used to restore GenTax fully in the event of a major disruption or outage.	**Not implemented**

As discussed in recommendation no. 9, DOR is currently developing a new disaster recovery solution. As such, no testing can occur until the solution is approved and implemented.

Recommendation #11

Request an independent security review of controls over servers operated by FAST Data Services.	**Not implemented**

As reported during the audit, DOR uses services provided by FAST Data Services. GenTax sends encrypted Oregon personal income tax return data to servers at an external data center where FAST Data Services analyzes them.

When GenTax was implemented, DOR security professionals discussed the security measures in place at the external data center, and stated they were satisfied with the stated controls. They also obtained a memo from FAST Data Services that outlined the methods used to ensure the data was secure.

However, our recommendation was that DOR obtain independent assurance of these controls, which would help ensure controls were implemented and operating effectively. DOR agreed with this recommendation, but declined to request an independent security review. Agency management indicated this topic may be revisited during future contract negotiations with the vendor.

Conclusion

DOR has made steady progress in addressing our findings and recommendations. The agency has improved its procedures to:

- ensure missing interface files are tracked and reviewed;
- identify which GenTax roles should not be combined;
- ensure proper written instructions are available to help managers request appropriate access for their employees to GenTax; and
- monitor certain actions taken by privileged users.

In a few areas, updates to procedures have only been proposed, but not yet fully approved and implemented, such as those relating to periodic manager review of user access.

DOR also identified potential solutions to help monitor execution of some of the new controls. Specifically, they plan to monitor activities taken by users having potentially conflicting roles and to enforce manager review of access. These technical solutions are not yet completed, but they represent good progress in addressing our recommendations, and go one step beyond simply developing new procedures.

DOR made no progress in implementing our final two recommendations. For disaster recovery testing, implementing the recommendation depends on the completion of other activities currently in progress. For recommendation no. 11, DOR had already expressed during the audit that they were satisfied with the stated security controls, and that contracting practices at the time the original contract was developed did not call for independent verification of security controls. The agency expressed then, as now, that they will revisit this topic during future contract negotiations.

Follow-up Report Team

Will Garber, CGFM, Deputy Director

Teresa Furnish, CISA, Audit Manager

Erika Ungern, CISA, CISSP, Principal Auditor

Sheila Faulkner, Staff Auditor

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

This report is intended to promote the best possible management of public resources.
Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits