State of Oregon

Oregon Department of Revenue: GenTax Accurately Processes Tax Returns and Payments, but Logical Access and Disaster Recovery Procedures Need Improvement

February 2018

Secretary of State
Dennis Richardson

Audits Division, Director
Kip Memmott

Report 2018 – 08

This page intentionally left blank.

Oregon Department of Revenue: GenTax Accurately Processes Tax Returns and Payments, but Logical Access and Disaster Recovery Procedures Need Improvement

Report Highlights

The Oregon Department of Revenue (DOR) designed and implemented controls in their GenTax system to provide reasonable assurance that tax return and payment information remains complete, accurate, and valid from input through processing and output. Logical access controls and change management controls are generally sufficient, but some areas need improvement. In addition, existing controls ensure the creation of appropriate backup of GenTax system files, though DOR does not have assurance they could timely restore the system in the event of a disaster or major disruption.

Background

The Oregon Department of Revenue replaced its legacy tax systems with GenTax, an integrated tax processing software package. This system processed about $10.3 billion in payments and $1.2 billion in refunds for tax periods ending in 2016.

Purpose

The purpose of our audit was to review and evaluate key application and general computer controls governing DOR's GenTax system. We focused on personal income, withholding, and corporate income and excise tax programs.

Key Findings

1. GenTax controls ensure accurate input of tax return and payment information for personal income, withholding, and corporate income and excise tax programs. Additional processing and output controls provide further assurance that GenTax issues appropriate refunds and bills to taxpayers for taxes due.
2. Logical access controls are generally sufficient, but DOR needs to make improvements to ensure managers have enough information to request appropriate access. DOR should also ensure that access remains appropriate for users who change jobs and is removed for users who are terminated.
3. DOR monitors and tracks changes to GenTax to ensure system developers implement only approved program modifications, but better guidance is needed for testing procedures to ensure program modifications meet business needs.
4. DOR does not have sufficient assurance that it could timely restore GenTax in the event of a disaster or major disruption.
5. DOR has not obtained independent verification that the GenTax vendor has implemented appropriate controls over servers at an external data center to provide additional assurance that Oregon data is secure.

Recommendations

The report includes 11 recommendations to DOR regarding needed improvements to logical access procedures, disaster recovery plans and tests, and independent assurance of controls over servers at an external data center.

DOR generally agreed with our recommendations. DOR's response can be found at the end of the report.

Secretary of State, Dennis Richardson
Oregon Audits Division, Kip Memmott, Director

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of his 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 and oversees audits and financial reporting for local governments.

Audit Team

Will Garber, CGFM, MPA, Deputy Director

Teresa Furnish, CISA, Audit Manager

Erika Ungern, CISSP, CISA, Principal Auditor

Sherry Kurk, CISA, Staff Auditor

Sheila Faulkner, Staff Auditor

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

website: sos.oregon.gov/audits

phone: 503-986-2255

mail: Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, Oregon 97310

We sincerely appreciate the courtesies and cooperation extended by officials and employees of the Oregon Department of Revenue during the course of this audit.

Oregon Department of Revenue: GenTax Accurately Processes Tax Returns and Payments, but Logical Access and Disaster Recovery Procedures Need Improvement

Introduction

The Oregon Department of Revenue (DOR) designed and implemented controls in their GenTax system to provide reasonable assurance that tax return and payment information remains complete, accurate, and valid from input through processing and output. Logical access controls and change management controls are generally sufficient, but some areas need improvement. In addition, existing controls ensure the creation of appropriate backup of GenTax system files, though DOR does not have assurance that they could timely restore the system in the event of a disaster or major disruption.

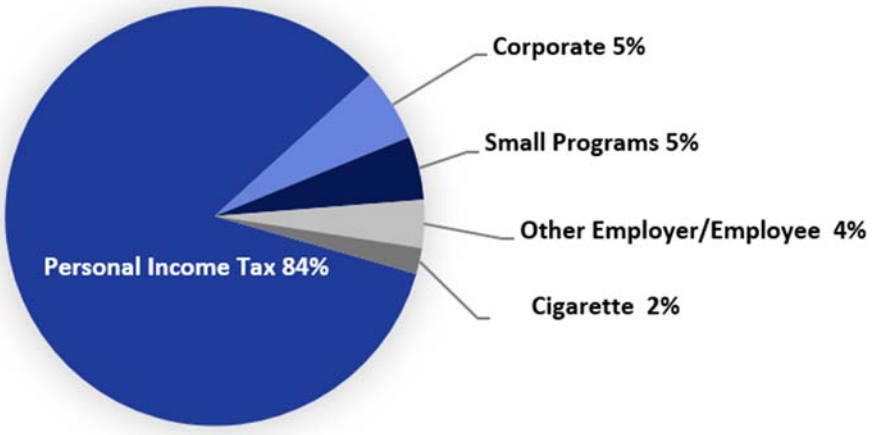
The Oregon Department of Revenue administers multiple tax programs

DOR administers over 30 tax programs, including the state's personal income, withholding, and corporate income and excise tax programs.

2015-17 Revenue

DOR projected $18.5 billion total tax revenue for the 2015-17 biennium. DOR transfers 91.4% of this revenue to the General Fund, 3.8% to counties, and 3.1% to other state agencies.

2015-2017 Revenues by Tax Program



Source: Oregon Department of Revenue 2015-2017 budget

DOR projected $18.5 billion total tax revenue for the 2015-17 biennium. DOR transfers 91.4% of this revenue to the General Fund, 3.8% to counties, and 3.1% to other state agencies. The remaining revenue supports DOR operations. The tax revenue DOR collects is comprised of 83.8% personal

income tax, 5.6% corporate taxes, 3.7% other employer and employee taxes, 2.0% cigarette taxes, and 4.9% from small programs such as inheritance taxes.

The GenTax system processes tax returns and payments

In 2013, DOR received initial project funding and approval for its Core System Replacement (CSR) project to implement GenTax, an integrated tax processing software package. GenTax replaced most of DOR's legacy core systems, which were built on aging and obsolete software applications and databases from the 1980s. The total cost of the CSR project as reported in the 2017-2019 Governor's Budget was $78 million, including debt funding and preliminary planning phases.

GenTax, a web-based, commercial, off-the-shelf product developed by FAST Enterprises, is used by 26 state revenue agencies nationwide, including Oregon. GenTax uses standardized core coding with configuration to meet individual state requirements.

DOR implemented GenTax in four major rollouts, with the fourth rollout completed in November 2017.

Source: Oregon Department of Revenue

DOR personnel continue to work closely with contractors from FAST Enterprises to develop and configure the system to meet Oregon's specific needs, as well as for production support. FAST Enterprises personnel will continue to provide on-site operational support through November 2021, based on the current contract.

Other agencies are also involved with GenTax operation and use. The Department of Administrative Service's (DAS) state data center houses the servers on which GenTax operates and DAS employees perform activities such as batch monitoring, server administration, and execution of backup routines. Some employees from the Oregon Employment Department and the Department of Consumer and Business Services also have limited access to GenTax, as DOR receives Oregon Combined Payroll payments then transfers the monies to tax programs at these other agencies.

Objective, Scope and Methodology

Our audit objectives were to determine whether information system controls at DOR governing the GenTax system provide reasonable assurance that:

- Selected tax program transaction data remain complete, accurate, and valid during input, processing, and output;
- System information is protected against unauthorized use, disclosure, modification, damage, or loss;
- Changes to computer code and configurations are managed to ensure integrity of the system and that only approved program modifications are implemented; and
- System files are appropriately backed up and can be timely restored in the event of a disaster or major disruption.

Our review of the GenTax application focused on the personal income, withholding, and corporate income and excise tax programs for tax periods ending in 2016. We reviewed input associated with tax returns and payments, and the processing and output activities associated with this data entry. Some tests of corporate taxes included tax periods during state fiscal year 2017, which ended on June 30, 2017. DOR implemented the withholding tax program in GenTax in November 2016, so most of our tests associated with withholding payments used converted data. Tests of refunds covered multiple tax periods. Together, the areas covered in this audit represented approximately 90% of the $10.3 billion in allocated payments and 98% of the $1.2 billion in refunds processed for tax periods ending in 2016.

We also reviewed logical access over the GenTax application and privileged access[1] to GenTax servers. For change management, we focused on maintenance changes to GenTax, as opposed to processes used for major project rollouts. Our review of backup and disaster recovery focused on procedures at DOR, not those of the DAS state data center, which executes backup routines for GenTax servers.

We assessed the reliability of GenTax data by reviewing documentation, evaluating high-level controls over processes to update database tables, and interviewing agency and contractor officials about the data and system. We obtained access to a backup database containing relevant data tables and performed queries to extract data for testing. We evaluated information in specific tables against information in other tables to assess data completeness and accuracy. In addition, throughout our testing procedures, we compared the data against source documentation and GenTax data from the production environment, as applicable. We

[1] DOR defines privileged access as any rights "elevated" beyond what the typical user receives, including administrative rights to servers.

determined that the data were sufficiently reliable for the purposes of this audit report.

We also conducted interviews with knowledgeable DOR staff and managers, observed processes and control procedures, and reviewed relevant policies and procedures. We also evaluated or tested:

- 1.9 million personal income tax returns for the 2016 tax year;
- 3.2 million W-2 records submitted by employers for tax periods ending in 2016;
- 0.8 million 1099R records for tax periods ending in 2016;
- 3.3 million refund records for all tax periods in GenTax;
- 3.6 million payment records for tax periods ending in 2016;
- 60 corporate tax returns and associated payment and withholding records out of a population of 83,297 corporate tax accounts for tax periods ending between July 1, 2016 and June 30, 2017; and
- groups, functions and account information associated with 1,479 GenTax user accounts.

We used the ISACA publication "Control Objectives for Information and Related Technology" (COBIT), and the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual" (FISCAM) to identify generally accepted control objectives and practices for information systems.

We conducted this performance 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 and reported provides a reasonable basis to achieve our audit objectives.

Audit Results: GenTax accurately processes tax returns and payments, but improvements are needed to strengthen logical access and disaster recovery procedures

DOR designed and implemented controls to provide reasonable assurance that tax return and payment information remains complete, accurate, and valid during input, processing, and output for the personal income, withholding, and corporate income and excise tax programs.

Logical access controls are generally sufficient to restrict GenTax access to appropriate users. However, we noted controls need strengthening to ensure managers have enough information to request appropriate access. Better controls are also needed to ensure ongoing access remains appropriate for users who change jobs and to ensure users who have left employment with DOR or with other entities have their access terminated timely.

Change management controls provide sufficient assurance that all program modifications receive approval prior to implementation. However, DOR needs to develop better guidance for testing procedures to ensure program modifications meet business needs and do not adversely affect other portions of the application.

Existing controls also ensure the creation of appropriate backups of GenTax system files. However, DOR does not have sufficient assurance that the system could be restored in a timely manner in the event of a disaster or major disruption.

Further, GenTax sends some taxpayer information to servers hosted at an external data center for fraud analysis. However, DOR has not obtained independent verification that the GenTax vendor has implemented appropriate controls over these servers to provide additional assurance that Oregon data is secure.

GenTax application controls ensure proper processing of tax returns and payments

Effective application controls include both manual and automated processes that ensure:

- Only complete, accurate, and valid information is entered into a computer system;
- Data integrity is maintained during processing; and
- System outputs conform to anticipated results.

We found the design and implementation of GenTax application controls provides reasonable assurance that tax return and payment information remains complete, accurate, and valid during input, processing, and output.

We focused on the personal income, withholding, and corporate income and excise tax programs.

Input and interface routines provide reasonable assurance that information is complete and accurate

Input controls should be in place to provide reasonable assurance that all authorized source documents and input files are complete and accurate, properly accounted for, and transmitted in a timely manner for input into the computer system. For GenTax, such controls help ensure that tax returns and payments received are completely and accurately entered, and associated accounts are credited appropriately.

DOR receives tax returns and payments by mail or through electronic methods, with the majority sent electronically. DOR implemented controls to ensure the accurate entry for both types.

The mail processing center receives paper tax returns and sends them to other business units for manual data entry or scanning. Data entry primarily takes place through several intake systems, which then send the information to GenTax via interface files. To ensure the appropriate entry of return data, DOR employees double enter the data and perform batch balancing to ensure they entered all returns received. GenTax production control processes monitor interface files from intake systems to ensure appropriate receipt of all expected files.

For payments received by mail, taxpayers identify where to apply their payment through payment vouchers. DOR employees batch, image, and balance paper checks and cash through an intake system, which interfaces the information to the bank and to GenTax. DOR's banking unit balances each batch to ensure accurate input occurred and reconciles bank deposits to GenTax. If taxpayers do not send payment vouchers with their paper payments, DOR's miscellaneous cash unit performs research and creates manual vouchers to apply the payments to the appropriate accounts.

Electronic tax returns are primarily processed through the Modernized eFile system that runs through a gateway with the Internal Revenue Service (IRS). Taxpayers submit returns electronically through commercial tax software, which sends the information to the IRS gateway. The IRS packages this information and sends it to a location where GenTax web services retrieve, open, and validate the tax returns. GenTax sends an acknowledgment back to the IRS to indicate whether the return was accepted or rejected. The IRS then provides this information to the software vendor, which should notify taxpayers, who are responsible for correcting and resubmitting their return if it was rejected.

DOR mainly receives electronic payments through Automated Clearing House (ACH) payment processes. Taxpayers initiate ACH payments, which must include specific instructions on how to apply the payment. DOR controls these ACH payments primarily through interface monitoring and by requiring payment headers to meet accepted formats. GenTax rejects

incorrectly formatted data. In addition, DOR performs monthly reconciliations between GenTax and Oregon State Treasury data to ensure that ACH and other payments match.

Automated processing routines accurately verify and edit returns and payments

DOR designed and implemented controls that provide reasonable assurance that GenTax corrects or identifies return and payment errors and routes them to employees to review and take action before further processing occurs.

Best practices indicate procedures should be established for data processing to help assure that data are processed completely and accurately, that data retains validity, and that appropriate data confidentiality is maintained during processing. Expected controls include applying edit and validation checks of data, suspending transactions with errors from further processing until corrected, and monitoring automated routines to ensure information is completely processed.

After receiving submitted returns and payments, GenTax validates the input, applies processing edits to ensure they meet expected formats and tax rules, and posts them to taxpayer accounts as needed. If GenTax identifies an error, different actions occur depending on the type of error encountered. For returns processing, GenTax automatically fixes some errors, such as math mistakes, and then continues processing the return. Other errors cause the return or payment to be suspended for review by DOR employees. GenTax places suspended items into work queues, which DOR managers use to set priorities and review whether suspended items are being resolved.

In addition, GenTax uses a series of risk rules to identify potentially fraudulent personal income tax returns. This process prevents a return from further processing until GenTax receives additional information that allows the return to pass the rules, or DOR employees manually release the return. This may delay the processing of refunds, but allows DOR to take actions such as verifying withholding or verifying the taxpayer's identity.

Our tests of data showed GenTax appropriately processed tax returns. For example, we concluded GenTax:

- Appropriately calculated taxes due based on the taxable amount identified on the return or as adjusted from other return processing routines;
- Verified that deductions, credits, and exemptions for personal income tax returns were appropriately applied and for the correct amounts, including those for the standard deduction, personal exemptions, federal tax liability amount, earned income credits, and the correct use of standard or itemized deductions;

- Checked that dependent totals for personal income tax returns were appropriate and that those who were claimed as dependents did not in turn claim dependents on their tax return; and
- Applied math edits to ensure totals used to calculate taxes, refunds, and tax-to-pay were appropriate.

GenTax and DOR employees verify that withholding reported by taxpayers matches external records

We concluded that GenTax and DOR employees reasonably ensure income tax withholding claimed by personal income taxpayers on their tax returns matches withholding records submitted by employers.

Employers submit W-2s and 1099s to DOR to report taxes withheld from their employees' paychecks. When filing tax returns, personal income taxpayers report the amount of withholding and submit W-2s and 1099s as support. GenTax performs matching routines to evaluate whether the claimed withholding matches what was reported by the employer. If GenTax cannot match the records according to business rules, the return is held until DOR receives additional information or a DOR employee manually releases it.

We confirmed the effectiveness of GenTax's matching routines and DOR procedures to verify withholding manually by comparing W-2s and 1099s submitted by employers to the withholding claimed by personal income taxpayers on their tax returns. Based on our review, we concluded that over 99.7% of personal income tax returns reported withholding that was adequately supported by W-2s and 1099s.

During our testing, we identified 3,427 Form 40 returns, or 0.2% of these returns, representing only 0.04% of withholdings for these returns, where the taxpayer claimed no withholding, but W-2 and 1099 records submitted by employers showed withholding for the taxpayer. DOR managers noted that GenTax was not configured to review withholding when the taxpayer does not claim it. As a result, these taxpayers did not receive credit for their withholding payments. According to DOR, taxpayers have the responsibility to file accurate tax returns. In these cases, the taxpayer made an error, and could amend their returns if made aware of the error. However, DOR does not issue any correspondence to taxpayers informing them that withholding existed that they did not report on their tax return.

Batch and interface monitoring ensure complete processing

GenTax processes nightly batches and interface files automatically and generates reports or alerts to identify errors. DOR has implemented controls to monitor and resolve batch and interface errors. These controls help ensure that errors are detected and resolved so that tax returns and payments are processed timely and accurately. While DOR has not been tracking resolution of all interface errors to ensure resolution and to identify repetitive errors, it has developed plans to begin this type of tracking.

During data processing, transactions may fail to process completely or accurately due to errors or inconsistencies in the data or system interruptions. To identify these instances, organizations should monitor batch processing and interfaces with other systems to ensure the receipt and processing of all transactions.

GenTax performs most processing during nightly batch processing[2] jobs. DOR established parameters for these batch processes and production control at the DAS state data center executes and monitors them. If a batch process fails, GenTax generates an event record known as an intervention to log the process in error, the server on which it occurred, and when the error occurred. Depending on the business rules established for a particular error, the intervention may cause the entire processing cycle to stop, requiring manual action to resolve the error and restart processing. However, GenTax usually allows processing to continue without halting the processing cycle. DOR monitors interventions daily and assigns them to developers for investigation.

DOR also monitors interfaces into GenTax. GenTax produces a daily report that identifies each interface processed that day and identifies errors encountered, including personnel assigned to resolve the error. We concluded most interface failures occur because GenTax did not process a file, which can be appropriate if there were no records for the specific interface for that day. Interfaces that process but experience other errors generate interventions, which personnel track separately.

Most interventions are resolved quickly, but some require additional manual actions, and may require resolution of an underlying issue to prevent future reoccurrences. Our review found 97.5% of all interventions logged in GenTax were resolved within three days. At the time of our review, all the interventions still open were tracked on a spreadsheet with most tied to open service tickets.

Our review of a selection of daily interface reports showed that management had assigned a developer or an analyst to review all identified missing files and errors. DOR has not been documenting resolution of missing interface files to ensure they were all resolved, but began planning to develop a process for this tracking at the end of our audit. Better documentation of interface errors could help identify possible patterns and ensure appropriate resolution for all missing files.

GenTax issued accurate refunds and bills for taxes due

GenTax controls provided sufficient assurance that taxpayers received accurate refunds. In addition, GenTax issued accurate bills for tax owed according to DOR's business rules.

---

[2] Batch processing is the execution of a series of jobs in a computer system without manual intervention.

Based on the processing of payments and tax returns, GenTax automatically produces multiple outputs, including refunds and correspondence to taxpayers, such as notices to taxpayers who did not pay the full tax due. As part of this process, GenTax automatically calculates the amounts and any associated interest or penalties related to the refund or the billing.

We tested the billing process and concluded:

- Correspondence to taxpayers included accurate tax due and interest and penalty calculations;
- Correspondence to taxpayers was sent according to the expected schedule; and
- Bill stages for collections actions were started according to the expected schedule.

If the combination of returns and payments indicates a refund is due, GenTax automatically generates a refund record and applies a series of risk rules that determine the level of approval required for the refund to be processed. Most refunds are automatically approved, but higher-risk refunds need approval by DOR employees through up to three levels of review.

Our testing of refunds showed:

- Refund amounts were appropriately calculated;
- All issued refunds were approved; and
- High-risk refunds were approved at appropriate levels, per risk rules, and by different individuals at each level.

GenTax logical access controls are generally sufficient but could be improved

GenTax logical access controls are generally sufficient, but DOR should make improvements to ensure the enforcement of segregation of duties, that managers have sufficient information to request appropriate access, and that ongoing access remains appropriate for users who change jobs or is removed for terminated employees. In addition, DOR needs to monitor the actions of users with privileged access to GenTax servers.

Access to computer systems should be restricted to each user's individual job requirements for viewing, adding, or altering information. Management should periodically review and confirm users' access rights to ensure they remain appropriate. Users who no longer need access should have their access rights terminated timely. In addition, organizations should specifically monitor the actions of users with elevated access, such as security administrators, to provide additional accountability.

Logical access controls are generally sufficient for most access

GenTax logical access controls are generally sufficient to ensure users are uniquely identifiable and appropriately authenticated, and that most access is appropriate.

DOR's procedures generally ensure that access is appropriately restricted and that actions taken tie back to a unique individual who performed that action. For example:

- Managers request access for their employees, which is then granted by a separate group of individuals;
- Unique user names are used to allow users and their actions to be identified;
- GenTax access to the production environment is automatically disabled after 120 days of non-use;
- GenTax maintains logs of user activities that may be reviewed if there are potential problems identified, such as a potential violation of privacy policies;
- GenTax automatically ends user sessions after a period of inactivity; and
- Users are locked out of GenTax after a specified number of failed login attempts.

Access and segregation of duties documentation needs improvement

As part of granting appropriate access, system owners should identify and prevent granting access to incompatible transactions. For example, the same user should not be able to create and approve a payment. In addition, those requesting access should have instructions to ensure they fully understand which access rights they are requesting.

GenTax uses role-based logical access with 153 groups attached to one or more of 415 defined functions. Managers should request access for their users based on the groups as documented within GenTax.

We found the documentation for most groups provided general information about the types of actions available for use by someone in the group. Some generic groups allowed access to multiple view only functions that we concluded represented an appropriate description. However, the descriptions of a small number of groups did not identify the functions included in that group.

In addition, DOR managers indicated that they discussed segregation of duties considerations when developing the roles and groups to prevent the combination of incompatible duties. However, DOR did not develop documentation identifying incompatible roles.

We also noted managers varied in how they requested access. Some requested groups, while others specified functions or a general type of access without specifying group or function. While most functions allowing

the ability to add or modify data were associated with only one group, some had multiple possible groups.

Without sufficient definition, documentation, and guidance to managers and access administrators, managers may inadvertently request access for users that exceeds what is required to perform job duties. In addition, without documentation of incompatible roles, managers may inadvertently request access to incompatible duties, resulting in improper segregation of duties.

Termination of access was not always timely

DOR has not adequately ensured that GenTax access ends promptly after employees leave DOR. Managers should request removal of access when employees leave, but DOR's review process does not ensure that timely access termination occurs.

Organizations should remove the access rights of all employees, contractors, and third-party users to system information upon termination of their employment, contract, or agreement. Failure to remove access timely increases the risk that inappropriate activity may occur.

When employees leave DOR, managers should request removal of GenTax access. Program coordinators review reports of terminated employees against a list of access requests to evaluate whether managers had requested access to be terminated. However, this process takes place approximately once per month, with no set schedule for the review. In addition, the review only evaluates requests, without verifying that access was removed.

In addition to access for DOR employees, DOR grants limited GenTax access to some employees from the Department of Consumer and Business Services (DCBS) and the Oregon Employment Department (OED). A DOR employee contacts these agencies monthly to ask whether users still require access. However, other external partners, such as DAS or FAST employees, also have access to GenTax but DOR managers have no formal regular review process to ensure the access is still required.

We reviewed the logical access accounts of 162 users whose employment with DOR, DCBS, or OED had ended and evaluated whether their access was timely removed. We found 11 users retained their access for more than 31 days after termination, indicating managers did not always request timely removal of access, and the manual review processes were not effective.

We also found three DOR employees, two OED employees and one external vendor who no longer required access to GenTax retained active GenTax group access even though their accounts were disabled. While these users could no longer log in, not ending the group access could result in inappropriate access if the user were to regain GenTax access. For example, users may leave DOR and later return in a different role where their access should be more restricted. If employees responsible for setting up the

renewed access do not notice that previous groups remain active, they may inadvertently grant excessive access.

Manager review of access is not formally required

DOR policy does not require managers to perform periodic reviews of access provided to users and DOR does not have processes in place for managers to perform or document ad hoc reviews.

Best practices indicate that system owners should periodically review and confirm users' access rights to ensure they remain appropriate.

Although DOR officials indicated that managers who request logical access to GenTax should periodically review the access provided, they have not developed written procedures for this review, and there is no requirement defined in the logical access policy. These weaknesses increase the risk that users will have more access to the system than they need to perform their duties, which could result in the compromise of the system or its data.

We evaluated access granted to users in eight groups that provided specialized abilities, such as the ability to approve refunds at different levels. There were 206 users with access to at least one of these groups. Of these, we found 19 users with inappropriate access for the user's current role. Most of these were due to the user having changed positions without appropriate updates to their access. For others, the user had access to perform functions in GenTax that they did not routinely perform, and, when questioned, managers indicated the access was inappropriate and should be removed.

In addition, we specifically reviewed access to five GenTax groups provided to 10 business users assigned to the GenTax project team. Three of these users had the ability to add, delete, and modify, which was not required for their current role on the project team. This access appeared to be an artifact of the access they would have had in their business units prior to joining the project team. In addition, six members of the project team had virtually unlimited access to GenTax production functions, with the ability to perform actions such as approving high-risk refunds. DOR management removed this ability when we identified this issue.

DOR does not monitor the activities of privileged users

DOR does not have a process to monitor the activity of GenTax privileged users. Privileged access enables an individual to take actions that may affect computing systems, network communication, system and user files, application data, and user accounts, including the creation and deletion of accounts.

Statewide information security standards indicate that agencies shall require servers to log security events.[3] In addition, controls should exist to

[3] Security events include actions that could alter the security of a system, such as policy changes or the creation of an access group with elevated privileges.

monitor the use of sensitive or privileged accounts to ensure only approved actions occur.

DOR follows procedures established by DAS to request privileged access to GenTax servers. This access has been granted to multiple personnel at DAS, as well as to individuals at DOR. Security personnel periodically monitor access assignments to the groups allowing privileged access to ensure they remain appropriate. Additionally, DOR managers reported they maintain logs of administrator activities.

However, there is no current process in place to monitor those logs. Failure to monitor the activities of privileged users increases the risk that unauthorized action may compromise GenTax and its data.

Change management controls are generally strong, but better guidance is needed for testing

Controls are generally sufficient to ensure that developers implement only approved program modifications. However, DOR needs to provide additional guidance on testing procedures to ensure program modifications meet business needs and do not adversely affect other portions of the application.

DOR staff tracks changes and sufficiently controls software versions

DOR employees adequately track changes to GenTax computer code and use software to ensure different versions of computer code are controlled. This software ensures the same user who made the change cannot promote the software code to the production environment.

Organizations should have formal change management processes and procedures to handle all requests for changes to applications. These procedures should ensure that organizations evaluate, approve, and track requests prior to implementation, and then review them against planned outcomes following implementation. This mitigates the risk of instability or damage to data in the production environment by providing assurance that developers promote only approved changes to production.

DOR has implemented and documented controls to assess, track, and evaluate change requests, and how DOR will make corrections, changes, and enhancements to GenTax computer code. For example, DOR:

- Formally defined responsibilities for the GenTax business and support teams;
- Implemented a tracking tool to log and track all GenTax changes;
- Developed processes to document, review, prioritize and authorize new solution requests (SQRs) for impact and effort;
- Developed processes to evaluate and approve completed changes, including requirements to compare modified code to existing code;

- Developed processes to roll back and rework an SQR if there is a failure during any stage of change;
- Implemented automated controls which require at least two levels of approval prior to promoting the modified code to production; and
- Implemented automated controls to prevent the employee who developed the code from promoting it to production.

Documentation of test expectations needs improvement

DOR personnel responsible for ensuring code or system changes meet users' needs have minimal guidance on tests to perform and documentation requirements. As a result, it is sometimes unclear what tests DOR performed and whether they were sufficient to ensure the solution meets business needs.

Best practices indicate organizations should establish test plans that define roles, responsibilities, and success criteria. Such plans should consider the risk of system failure and implementation errors, and should include requirements for performance, stress, usability, pilot, and security testing.

DOR provides some guidance regarding testing of SQR changes. It includes general descriptions of the type of testing developers and business analysts should perform. The business analysts are responsible and accountable for reviewing each request, verifying the problem or enhancement, gathering business requirements, proposing or confirming a solution, developing and performing functional and user acceptance tests, maintaining and providing training, and coordinating legislative fiscal impact requests.

However, business analysts have little guidance or criteria to meet these responsibilities and ensure adequate testing and documentation occur. In particular, DOR has not developed standard test plan formats for routine changes, or specified the required level of documentation of tests performed and their results. We also noted inconsistencies in the level of documentation for change requests. We concluded this was partly due to the absence of documented guidance and standard plans and partly due to changes to the requirements associated with SQRs as DOR shifted focus from the project to operations.

Lack of guidance or criteria documenting the types of test plans required for different changes may result in changes not meeting the needs of the business users.

GenTax may not be timely or completely recovered in the event of a disaster

Controls are sufficient to ensure that DOR appropriately backs up GenTax system files. However, DOR does not have assurance that they could timely restore GenTax in the event of a disaster or major disruption.

Restoring computer applications after a disaster or serious disruption requires significant advance planning, coordination, and testing. This strategy should ensure the copying of all critical computer files to an off-site location as frequently as needed to meet business requirements. Organizations should also document disaster recovery procedures in a disaster recovery plan and periodically test the plan to ensure effectiveness.

DOR's GenTax servers reside at the DAS state data center. DAS and DOR share responsibility for recovering these systems in the event of a serious disruption.

We evaluated DOR's process for backing up GenTax, including backup frequency, notification for backup success or failure, recovery priority of business critical tasks, and whether or not backups are tested on a periodic basis. We found DOR has a process in place to ensure that GenTax system files are backed up locally and is verifying that required files are being backed up to off-site storage. However, DOR has not tested the process to restore the GenTax application and data files using the off-site backups.

In addition, we noted that DOR has not developed a disaster recovery plan for GenTax for incorporation into their agencywide business continuity plan. Because of this, DOR does not have assurance that it could restore the system and its data in the event of a major disruption or outage.

The lack of a disaster recovery plan is partially due to the status of GenTax as a new computer system for DOR. DOR was also in the process of updating their agencywide business continuity plan during the audit, as the existing version was created before GenTax was implemented. DOR indicated it was working on updating the plan to include GenTax.

DOR has not obtained independent assurance of FAST Data Services controls

DOR has not gained independent assurance that FAST Data Services has implemented appropriate controls over servers at an external data center housing Oregon personal income tax data.

Best practices indicate that when information is processed by external information systems, organizations should verify that required security controls on those external systems are appropriate. This verification can be achieved by third-party, independent assessments of those controls. Entities providing such assurance should be independent of the organizations whose controls are being assessed. We have noted this to be an emerging issue in many organizations using external entities to host or process their data. Currently, there are no DOR policies developed to address security requirements for this type of service.

As part of personal income tax return processing, DOR utilizes services provided by FAST Data Services, which, along with FAST Enterprises, is a

subsidiary of FAST LP. GenTax sends encrypted Oregon personal income tax return data to servers at an external data center where FAST Data Services analyzes them and assigns a risk score. FAST Data Services owns and maintains the servers. DOR did not obtain independent verification that the controls governing these servers are in place and functioning as designed.

DOR security professionals stated they discussed the security measures in place with FAST Data Services security personnel and were satisfied with the stated controls. DOR also obtained a memo from FAST Data Services that outlines what they reference as well-defined methods and best practices to ensure data is secure. Our review of this document did not reveal any weaknesses, and we saw no indication that the vendor has not implemented the stated controls. However, DOR did not request an independent security review to provide independent assurance that the internal controls and practices identified by the vendor function as intended. An independent review of the organization would provide additional assurance to DOR that Oregon data is secure.

Recommendations:

To improve application controls, we recommend DOR management:

1. Consider notifying taxpayers claiming no withholding if withholding records are found; and
2. Implement controls to track and analyze how interface file failures are resolved.

To strengthen logical access controls, we recommend DOR management:

3. Identify and document which GenTax roles should not be combined with others;
4. Fully document GenTax groups and functions and ensure managers have received instructions on how to request access;
5. Improve procedures to ensure user access is removed timely and completely when no longer needed;
6. Update policy to require periodic manager review of logical access granted to GenTax and develop a mechanism to enforce and document the review; and
7. Implement monitoring of logs to identify inappropriate activity taken by server administrators.

To strengthen change management procedures, we recommend management:

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

To strengthen disaster recovery procedures, we recommend management:

9. Develop and maintain a written disaster recovery plan for GenTax; and
10. Periodically test backups stored off-site to ensure they can be used to restore GenTax fully in the event of a major disruption or outage.

To provide additional assurance that personal income tax data is protected, we recommend management:

11. Request an independent security review of controls over servers operated by FAST Data Services.