Secretary of State Audit Report

Jeanne P. Atkins, Secretary of State

Gary Blackmer, Director, Audits Division

Oregon Employment Department: Computer Programs for Unemployment Tax Returns and Claims Need Attention

Executive Summary

Oregon Employment Department computer programs correctly process most individual unemployment insurance claims and associated employer tax returns, but these outdated computer programs should be replaced. Additional work is also needed to improve security, processes for changing computer code, and disaster recovery capability.

Computer programs correctly handle most unemployment benefit claims and tax statements, but should be replaced

Computer programs to handle unemployment claims and tax are inflexible, poorly documented, and difficult to maintain.

Oregon Employment Department (Employment) computer systems handle routine unemployment claims accurately. Systems also process most employer quarterly unemployment tax returns appropriately. However, due to system limitations, Employment staff must identify and manually correct some unemployment claim errors. In addition, some unemployment tax returns bypass automated routines that provide needed scrutiny to detect and correct errors.

These computer programs are inflexible, poorly documented, and difficult to maintain. Considering these factors, Employment should take steps to replace them with more robust and maintainable computer code.

Computer security problems increase risk that data could be compromised

Coordinated use of multiple security components is necessary to protect the integrity of computer systems and their data. Although Employment management and the state's data center have done much to protect Employment's computer systems, improvements are needed.

Areas of most concern include ensuring users have the appropriate level of access to computer programs, monitoring actions of users having the most powerful access to systems, and addressing state data center security weaknesses we identified in previous audits.

Processes to better control changes to computer code are needed

Our 2003 and 2012 audits noted problems managing programming changes to these systems. These conditions remain largely unchanged, and increase the risk that programmers could introduce unauthorized or untested changes to the system.

Although these weaknesses are long-standing, Employment managers and staff recently began work to resolve them. They currently have a project to acquire a software solution that could significantly enhance their ability to address many of the identified problems.

Disaster recovery capability is greatly improved, but Employment should ensure plans and processes are complete

Responsibility for recovering the use of computer systems in the event of a disaster is shared with the state data center where these computer systems are hosted. In 2014, the data center entered into an agreement with the state of Montana to place copies of Oregon's computer systems and data inside Montana's data center.

This innovative approach to disaster recovery significantly improves Employment's ability to resume operations in the event of a disaster but additional work is needed to ensure these systems and data are secure and can be made fully operational when needed.

Recommendations

We recommend that management take steps to improve processes for detecting and correcting unemployment tax return errors, improve system documentation, resolve security weaknesses, and fully develop and test disaster recovery procedures.

Agency Response

The agency's response to the report is included at the end of the audit report.

Background

The Oregon Employment Department uses OBIS to process unemployment insurance claims and OATS to process unemployment tax reports from employers.

The Oregon Employment Department (Employment) was created in 1993. One of its missions is to “support economic stability for Oregonians and communities during times of unemployment through the payment of unemployment benefits.” To achieve this mission, Employment’s Unemployment Insurance Division Benefits section provides partial wage replacement to eligible unemployed workers.

Employment pays unemployment insurance benefits primarily from the Oregon Unemployment Insurance Trust Fund. This money comes from unemployment taxes paid by Oregon employers. Employment determines employers’ tax rates according to legally defined state unemployment tax schedules. It also considers the age of the employer’s business and how many of its employees have drawn unemployment benefits.

Employment uses several computer systems to administer the unemployment insurance program. The Oregon Benefit Information System (OBIS) processes initial and ongoing unemployment insurance claims. In calendar year 2014, Employment paid about $625 million in unemployment insurance benefits through this system.

The Oregon Automated Tax System (OATS) collects and processes quarterly unemployment tax reports submitted by employers, determines whether the appropriate tax was paid, and bills employers for taxes still owed. In addition, the system processes refunds to employers. This system processed about $1 billion in tax receipts during calendar year 2014.

Accurately processing unemployment claims and employer tax statements requires inputs from several key sources. The unemployment insurance program requires those submitting claims for unemployment benefits to provide accurate and complete information, and employers to report their employees’ individual wages accurately.

Employment has used OBIS and OATS since the early 1990’s. These mainframe computer programs are located at the state’s data center administered by the Department of Administrative Services.

Audit Results

Computer programs correctly process most unemployment benefit claims and tax statements, but should be replaced

Employment's computer systems process and pay routine unemployment claims accurately and timely. They also ensure most quarterly unemployment tax returns are appropriately processed. However, procedures to identify and manage some unemployment claim errors are largely manual due in part to system limitations. In addition, some unemployment tax returns bypass a key system data validation routine. Last, staff does not use an important report that could help them detect and resolve some potential unemployment tax return errors.

These computer programs are inflexible and poorly documented. They are also difficult to maintain because they are written using an outdated programming language. Considering these factors, Employment ultimately will need to replace its unemployment insurance computer systems with a more robust and maintainable solution.

Unemployment insurance claims are processed appropriately, but further automation is needed

Transactions processed through computer systems should go through manual and automated procedures to ensure they are appropriate. In particular, procedures should ensure only complete, accurate and valid information is entered into a system, data integrity is maintained during processing, and system outputs meet expected results.

Employment uses a variety of automated and manual procedures to ensure OBIS processes routine unemployment insurance payments properly. These include automated routines to ensure data meets expected formats and to identify claims with potential problems. Our tests of claims data found that OBIS accurately calculates benefit amounts and generates benefit payments that meet requirements established in state law.

Although these processes and procedures are sufficient for normal processing, OBIS is not flexible enough to efficiently handle additional requirements, such as those that occurred during the latest economic downturn. To compensate for this weakness, Employment staff created additional reports outside of OBIS to identify potential errors. Resolving these errors requires staff to manually confirm the anomalies identified by the reports and correct them. This workaround may be difficult to execute in the event of an economic downturn, since Employment may not have the additional staffing required to handle the increased volume and complexity of errors.

Most employer tax returns are processed appropriately, but some procedures are bypassed

Employers submit quarterly unemployment insurance tax returns using two different forms. One form contains a detailed list of employees that includes their name, Social Security number, and wages paid. The other contains summarized payroll figures and additional tax information needed by other entities, such as the Oregon Department of Revenue. Employment uses the information from these tax forms to validate unemployment insurance claims and ensure unemployment insurance taxes are paid appropriately.

To ensure OATS processes unemployment tax returns properly, Employment uses automated and manual procedures. For example, Employment has processes to ensure payments received are accurately applied to employer accounts and to recalculate the tax due according to established tax rates.

Another procedure validates employers' tax returns by comparing detail and summary amounts. However, Employment modified the program code to bypass this comparison to avoid processing delays for a large payroll service provider that reports about 25% of all wage records. When this accommodation was no longer needed, management indicated that sufficient technical staff were not available to reverse the changes. Without this comparison, there is a greater potential that Employment will not detect overpayment or underpayment of unemployment taxes.

To identify instances when employers may have over or under reported taxable wages, OATS also generates a report that analyzes the wage data employers report each quarter. However, Employment managers indicated they are not using this report because it requires significant staff time to validate and respond to the potential errors. This task is further complicated because Employment does not require employers to disclose details regarding their calculation of taxable wages. By not using the report, staff did not detect that nearly 2,000 employers collectively overpaid their taxes by approximately $850,000 in 2014. One employer, a non-profit, overpaid its taxes by about $17,000, or 22 percent more than they actually owed. In addition, because Employment staff did not follow up on potential exceptions included in the reports, they did not detect that about 4,400 employers may have collectively underpaid their taxes by as much as $2.9 million. While these weaknesses indicate the need for improved processing, the associated errors represent only 0.4 percent of total taxes collected.

Systems are dated, inflexible, and poorly documented

Oregon's economy and the related unemployment rate changes over time. When significant increases in unemployment occur, such as those that occurred during the last economic downturn, Employment may be required to rapidly alter the way it processes unemployment claims to handle the increased volume.

Employment's computer systems were initially developed over 20 years ago and use an outdated computer programming language. Agency managers describe the systems as inflexible, making programming changes time-consuming and often impractical. As a result, they have implemented multiple workarounds outside of the systems to manage program changes and to better meet agency needs.

Documentation of these computer systems is also inadequate. Employment staff indicated that existing system documentation has not always been updated when changes occur, and that answering questions regarding system functionality would require staff to analyze program code. One result of poor system documentation is that Employment staff do not have a complete understanding of the system's security functions.

Computer security problems increase risk that data could be compromised

Proper security requires coordinated use of multiple security components to protect the integrity of computer systems and their data. The security industry refers to this methodology as defense in depth. The underlying principle is that it is more difficult to defeat a complex and multi-layered defense system than to penetrate a single barrier.

Since Employment's computer systems are hosted at the state's data center, responsibility for different parts of security is shared between these two organizations. Although Employment management and the state's data center have provided important protection measures for OBIS and OATS, improvements are needed to better secure these computer systems and their data.

Access to computer systems should be restricted according to each user's individual need to view, add, or alter information. Management should periodically review and confirm users' access rights to ensure they are appropriate. Users with powerful access, such as security administrators, should be specifically monitored to provide additional accountability.

Employment has processes for establishing users' access to computer systems, but these procedures do not ensure each individual's access is appropriately restricted. In addition, Employment staff does not independently monitor the actions of the users having the most powerful access to system functionality. Specific weaknesses include:

- Employment has not clearly documented how the various logical access methods work to limit users' access.
- Managers responsible for requesting and approving access rights for their staff are not fully aware of the extent of access they are authorizing.
- Managers do not periodically review and validate their staff's access privileges.

- System programmers have excessive and unmonitored access to enter or modify claims transactions.
- Employment does not appropriately restrict access to OATS and OBIS reports.

These weaknesses make it difficult to determine which users have access to specific resources or to validate whether users' access is appropriate. Since Employment systems contain mission critical and confidential information, they must be strictly protected from outside and inside threats. By not adhering to best security practices, Employment increases the risk that the system and its data could be compromised.

Related data center weaknesses increase risk

Our recent audit of the state's data center also identified security weaknesses that increase the risk that Employment's computer systems could be compromised. These weaknesses include or involve significant security components including:

- System configurations were not adequately managed.
- Monitoring and managing users with special access was inadequate.
- Critical network monitoring devices were not fully functional.
- Obsolete network equipment was not replaced.
- Potential security incidents were not adequately tracked.

We noted that the Governor, Legislature and the state Chief Information Officer have taken the first steps to address long-standing security weaknesses, but these solutions will take time, resources and cooperation from state agencies.

Although Employment management is not directly responsible for data center operations, it has not formally established security requirements with the data center or confirmed that these expectations are being met.

Processes to better control changes to computer code are needed

Computer program code should be strictly managed to ensure only tested and approved modifications are placed in production. To ensure this occurs, logical access to code should be strictly limited and monitored. Proposed changes to code also should be independently tested and compared to the latest approved version to ensure only appropriate modifications have been made. In addition, procedures to document key system design requirements and specifications should be in place.

Previous audits have noted weaknesses in this area, and we found only minimal improvement during the current audit. The program change control weaknesses posing the most significant risk included the following:

- Multiple programmers can modify programming code in the production environment.
- Adequate documentation of automated system controls or design specifications did not always exist.
- Programmers were not always required to create testing plans for changes to program code.
- Technical staff did not always perform independent reviews of computer code changes, including comparing modified code to approved versions, to ensure modifications were appropriate.
- Version control procedures were not in place to ensure approved and tested code would remain unaltered.

Collectively, these weakness increase the risk that Employment programmers could introduce unauthorized or untested changes to the system. Should this occur, Employment could experience costly errors or delays in processing individuals' unemployment benefit payments.

Although these weaknesses are long-standing, we noted that Employment management and staff is working to resolve them. They are planning to acquire a software solution which could significantly enhance their ability to resolve some of the identified problems.

Disaster recovery capability is greatly improved, but Employment should ensure plans and processes are complete

Restoring data center operations after a disaster or serious disruption requires significant advance planning, coordination, and testing. This strategy should ensure all critical computer files are copied to an offsite location as frequently as needed to meet business requirements. Disaster recovery procedures should also be well-documented and periodically tested to ensure they will function as planned.

Employment's mainframe computer systems are housed at the Department of Administrative Service's data center. Responsibility for recovering these systems in the event of a serious disruption is shared between the two agencies. In 2014, the data center entered into an agreement with the state of Montana to allow the data center to copy its mainframe computing environment to hardware located inside Montana's data center.

This innovative approach to disaster recovery is a significant improvement over prior plans, but some details and important tasks remain undone. One of the most important is for Employment to gain better assurance that computer code and data at the Montana site will remain secure. Employment also needs to update and test its disaster recovery procedures to ensure Employment and data center staff can successfully transfer its computer system operations to the Montana site.

Without fully updated and tested plans, Employment may not be able to quickly recover its critical technology infrastructure in the event of a disaster. In addition, gaining assurance that data stored at the offsite location is secure is imperative.

Recommendations

We recommend that Employment management:

- Improve documentation of OBIS and OATS system design and controls including processes for assigning and modifying users' logical access.
- Improve processes for detecting and correcting unemployment insurance tax return errors.
- Establish processes for regularly evaluating users' logical access to ensure it remains appropriate.
- Remove programmers' logical access to production screens and further restrict their access to the production environment.
- Implement procedures to log and monitor actions of those having powerful access to system functionality to ensure better accountability.
- Appropriately restrict access to OATS and OBIS reports.
- Establish security expectations with the data center and implement procedures to ensure those expectations are met.
- Improve processes for testing, evaluating, and documenting computer code changes and continue efforts to implement software to manage computer code.
- Fully develop and test disaster recovery procedures and ensure data stored at the offsite location is secure.
- Prepare for replacing OBIS and OATS with more flexible solutions.

Objectives, Scope and Methodology

The purpose of our audit was to review and evaluate the effectiveness of key general and application controls over the computing environment at the Oregon Employment Department (Employment). Our specific objectives were to determine whether:

- Information system controls provide reasonable assurance that employer tax and unemployment insurance claims transactions remain complete, accurate and valid during input, processing and output.
- Information systems and data are protected against unauthorized use, disclosure, modification, damage, or loss.
- Changes to computer code are appropriately controlled to ensure integrity of information systems and data.
- Information system files and data are appropriately backed up and can be timely restored in the event of a disaster or major disruption.

The scope of our audit included selected portions of the Oregon Automated Tax System (OATS) and the Oregon Benefit Information System (OBIS). These included processes for collecting and recording employer quarterly tax statements, unemployment insurance claims processing, and resolving administrative decisions. We included information system controls that were in effect through October 2015.

During the audit, we conducted interviews with Employment personnel, observed Employment operations and procedures, and examined available system documentation. To fulfill our audit objective, we evaluated or tested:

- unemployment claim data for months between January 2014 and April 2015 and Unemployment Tax reports and data from calendar year 2014;
- processes Employment staff used to provide access, access granted to selected users, and associated documentation relating to security systems;
- logical access provided to computer code and supporting documentation for selected changes; and
- backup schedules, restoration plans, and the results of disaster recovery tests.

We used the IT Governance Institute's publication "Control Objectives for Information and Related Technologies" (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 objective. We believe that the evidence obtained and reported provides a reasonable basis to achieve our audit objectives.

Auditors from our office, who were not involved with the audit, reviewed our report for accuracy, checking facts and conclusions against our supporting evidence.

Oregon
Kate Brown, Governor

Employment Department
875 Union St NE
Salem, OR 97311
503-947-1394
TTY-TDD 711
www.Employment.Oregon.gov

December 22, 2015

Neal Weatherspoon, IT Audit Manger
Audits Division
Office of the Secretary of State
255 Capitol St. NE, Suite 500
Salem, Oregon 97310

RE: Audit Report, Computer Programs for Unemployment Tax Returns and Claims Need Attention

Dear Mr. Weatherspoon,

Thank you for providing the Oregon Employment Department (OED) with the audit report noted above. We appreciate the work of the Oregon Audits Division staff and are pleased to have the recommendations in the report to help guide us in the future.

This is OED's response to the findings and recommendations contained in the above referenced audit report.

Finding 1: Improve documentation of OBIS and OATS system design and controls including processes for assigning and modifying users' logical access.

The agency agrees.

We are in the process of preparing to modernize our computerized systems. Work efforts are focused on documenting OBIS and OATS functionality to determine what will be needed for Unemployment Insurance (UI) Modernization which is a multi-year project.

A high level application portfolio document for OBIS and OATS mainframe applications were completed earlier this year and we have initiated the process of creating system documentation. A senior technical writer is working with the team to create the required documentation and is expected to complete this work by July 2017.

The security team has started creating logical access documentation along with input from the Mainframe Team. The access is limited in design due to old code and setup, where restrictions are in place by office rather than user. The existing system was created over twenty years ago based upon standards at that time. Another layer of complexity added to the system was a custom built program to add an additional layer of program security that is poorly documented. Staff with institutional knowledge of the program has long since retired. This will have to be addressed in Modernization.

Finding 2: Improve processes for detecting and correcting Unemployment Insurance tax return errors.

The agency agrees.

The Employment Department worked with the large payroll service provider referred to in the audit, which reports about 25% of all wage records, to address how those wage records are filed. Effective starting with the filings for the third quarter of 2015, the wage summary and wage detail parts of these filings are compared to identify potential tax return errors. The Employment Department is also pursuing options to ensure taxable wages are appropriately reported. While longer term options being pursued include automated computation of taxable wages, OED is committed to identifying shorter term solutions that, although more manual and resource intensive, may permit additional validation of correct taxable wage reporting.

Finding 3: Establish processes for regularly evaluating users' logical access to ensure it remains appropriate.

The agency agrees.

The Employment Department Information Security Team has been conducting a review of all user account access. They are working with program management to ensure that staff have the rights required to perform their job duties. Any unnecessary rights are being removed. All unused accounts are being purged from the systems. Policies and procedures related to access management will be developed.

Long term planning for the agency has the role of Access Management moving from the Information Security Team to another area, creating separation of duties and the ability for the Security Team to objectively review whether the procedures and policies related to account management are being followed.

Finding 4: Remove programmers' logical access to production screens and further restrict their access to the production environment.

The agency agrees.

The current access setup is limited in design, where restrictions are in place by office rather than user. This will have to be addressed in Modernization. The issue with restricting the access is because the system is old; the only way to fix the errors is for someone to go in and do that. So removing access is removing the way to fix these error records. Until modernization happens this will be an issue we might have to live with.

All rights to source code on the mainframe have been reviewed; any staff with rights who are not approved have had their rights to the source code terminated. This will be combined with the Source Code Management (SCM) project to ensure this is controlled in the future. Limited access to production code is necessary when fixing production issues after normal business hours.

Finding 5: Implement procedures to log and monitor actions of those having powerful access to system functionality to ensure better accountability.

The agency agrees.

All access identified in the previous confidential letter will be used in future efforts to limit access to only that which is required to perform job duties. In addition, we have an ongoing project to implement SCM which will provide additional layers of security.

The security and mainframe team have started documenting access of all users and developers on the OBIS and OATS application. Reports or a process will have to be created. The logging is at the CICS level and not at the file level, which is what will truly allow monitoring actions.

The Information Security Team will be implementing a Security Event and Information Management (SEIM) system this biennium. This will provide better monitoring and alerting of events and also will provide better log management and review. Unemployment Insurance will work with IT to determine what access should be monitored and tracked.

Finding 6: Appropriately restrict access to OATS and OBIS reports.

The agency agrees.

Unemployment Insurance has a work effort pending to restrict access to the service request system. Request for OATS and OBIS reports are submitted through the service request system. It's our intention to have all requests for reports run through UI. These requests will be reviewed and approved or denied by UI Management. The security and mainframe teams will coordinate to set these expectations with Enterprise Technology Systems (ETS).

Finding 7: Establish security expectations with the data center and implement procedures to ensure those expectations are met.

The agency agrees.

The Employment Department will work to share agency security requirements with ETS for future security needs. In addition, OED has begun implementing our own security controls to complement the ETS security and provide a better defense in depth for our systems and data.

Three of the controls included in the Security Policy Option Package are currently in the process of being implemented: Mobile Device Management, End Point Security and Multi-factor Authentication.

In addition, we are participating on a multi-agency committee with ETS to design and implement improved patch management. The OED is also addressing patch management internally.

The Employment Department has recently moved to the new firewall solution provided by ETS, this solution has been configured and implemented by the vendor. ETS continues to have the vendor under contract and on site to assist with the management and configuration of the firewall and its associated services.

Enterprise Technology Systems security has moved to the Enterprise Security Office (ESO) for the State. As that transition continues, we anticipate the security program for ETS will continue to mature and standardized, repeatable processes will be established and followed. Currently several are under review and modification, including the Incident Response Policy and Procedure.

Finding 8: Improve processes for testing, evaluating, and documenting computer code changes and continue efforts to implement software to manage computer code.

The agency agrees.

To address the current weaknesses on code changes, OED is well under way on a project to implement a version control system for mainframe application source code using CA Endevor. It is expected as per latest weekly reports that this tool will be fully functional by year end of 2016.

In addition, evaluation for adopting a Software development lifecycle which is a good fit for the current setup of OED IT and Applications is being done.

The Employment Department Quality Assurance Program has been established and is successfully implemented. The Program has developed a charter, guidelines, test plan templates, testing procedures, testing methodology and implemented a testing tool. The Program will continue to expand and mature over time, we expect to add at least one additional position to the team in the next six months.

Finding 9: Fully develop and test disaster recovery procedures and ensure data stored at the offsite location is secure.

The agency agrees.

The Employment Department recently adopted the DAS COOP (Continuity of Operations Plan) in effort to improve the agency Business Continuity Plan (BCP). Previous plans encompassed detailed actions surrounding issues that would be resolved within 72 hours. These plans are site specific and each OED physical location is expected to have their own plan.

The COOP deals with situations that interrupt OED's business functions for greater than 72 hours and would usually impact a significant part of the agency. The Disaster Recovery Plan is exclusive to IT and could be invoked during a BCP or Disaster Recovery event. Information Technology is currently in the process of updating all Disaster Recovery plans.

At this point, we have identified what are the agencies Mission Essential Functions. Based on this information a group of employees representing all programs of the agency have come together and developed the beginnings of the COOP. We are taking a different approach from the past BCP in that this plan is a comprehensive, all-hazards approach to incident management across a spectrum of activities.

Once the COOP plan has been finalized and approved by Executive Management, the agency will test to ensure data stored offsite is secure and can be recovered in the event of a disaster.

Finding 10: Prepare for replacing OBIS and OATS with more flexible solutions.

The agency agrees.

The Employment Department is currently in the planning and development phase for UI Modernization.

The Employment Department management appreciates your audit team's efforts and for the recommendations made in the audit report. We look forward to working with the Secretary of State's Audit Division in the future. If you have any questions or need further information, please contact Lisa Upshaw, Chief Audit Executive, at 503-947-3015.

Sincerely,

Lisa Nisenfeld
Director

Cc: Salvador Llerenas, Deputy Director, Employment Department
Erika Ungern, Principal Auditor, SoS Audits Division
David Gerstenfeld, Unemployment Insurance Director, Employment Department
Bill Truex, CIO, Employment Department
Annalise Famiglietti, Interim Deputy CIO, Employment Department

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of her office, Auditor of Public Accounts. The Audits Division exists to carry out 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 audits all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

Audit Team

William Garber, CGFM, MPA, Deputy Director

Neal Weatherspoon, CPA, CISA, CISSP, Audit Manager

Erika Ungern, CISA, Principal Auditor

Matthew Owens, CISA, MBA, Senior Auditor

Sherry Kurk, Staff Auditor

This report, a public record, 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

The courtesies and cooperation extended by officials and employees of the Oregon Employment Department during the course of this audit were commendable and sincerely appreciated.