



A REPORT
TO THE
MONTANA
LEGISLATURE

INFORMATION SYSTEMS AUDIT

*Data Integrity of the
Status, Tax Accounting,
Audit, and Rating System
(STAARS)*

Department of Labor and Industry

SEPTEMBER 2016

LEGISLATIVE AUDIT
DIVISION

16DP-01

INFORMATION SYSTEMS AUDITS

LEGISLATIVE AUDIT COMMITTEE

REPRESENTATIVES

RANDY BRODEHL, CHAIR
Randybrodehl57@gmail.com

TOM BURNETT
Burnett.tom@gmail.com

VIRGINIA COURT
virginacourt@yahoo.com

DENISE HAYMAN
Rep.Denise.Hayman@mt.gov

KENNETH HOLMLUND
rep.ken.holmlund@mt.gov

MITCH TROPILA
tropila@mt.net

SENATORS

DEE BROWN
senatordee@yahoo.com

TAYLOR BROWN
taylor@northernbroadcasting.com

MARY McNALLY, VICE CHAIR
McNally4MTLeg@gmail.com

J.P. POMNICHOWSKI
pomnicho@montanadsl.net

BRUCE TUTVEDT
tutvedt@montanasky.us

GENE VUCKOVICH
Sen.Gene.Vuckovich@mt.gov

MEMBERS SERVE UNTIL A
MEMBER'S LEGISLATIVE TERM
OF OFFICE ENDS OR UNTIL A
SUCCESSOR IS APPOINTED,
WHICHEVER OCCURS FIRST.

§5-13-202(2), MCA

FRAUD HOTLINE
(STATEWIDE)
1-800-222-4446
(IN HELENA)
444-4446
ladhotline@mt.gov

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Members of the IS audit staff hold degrees in disciplines appropriate to the audit process.

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

AUDIT STAFF

MIKI CESTNIK

DIEDRA MURRAY

Reports can be found in electronic format at:
<http://leg.mt.gov/audit>

LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel



Deputy Legislative Auditors:
Cindy Jorgenson

September 2016

The Legislative Audit Committee
of the Montana State Legislature:

This is our information systems audit of the Status, Tax Accounting, Auditing, and Rating System (STAARS) managed by the Unemployment Insurance Division in the Department of Labor and Industry (department).

This report provides the legislature information about data integrity involved in Unemployment Insurance contribution system processes. This report includes recommendations for improvements related to access management, data accuracy, and system changes.

We wish to express our appreciation to department personnel for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

TABLE OF CONTENTS

Figures and Tables.....	ii
Appointed and Administrative Officials	iii
Report Summary	S-1
CHAPTER I – INTRODUCTION AND BACKGROUND	1
Introduction	1
Background.....	1
Audit Scope and Objectives	2
Methodology.....	3
Overall Summary and Report Organization.....	3
CHAPTER II – USER ACCESS MANAGEMENT	5
Introduction	5
Improving Documentation and Defining Responsibility for the Access Management Process	5
Access Documentation Problems Were Identified for the Majority of Users Sampled.....	5
Periodic Monitoring of System Access Is Not Occurring.....	6
Improvements Needed in Defining and Monitoring User Access Roles and Privileges	7
Over-Assigned User Privileges Exist.....	8
Monitoring of Privileged Users Should Occur	9
CHAPTER III – DATA INTEGRITY REVIEW	11
Introduction	11
Manual Data Input and Adjustments	13
North American Industry Classification System (NAICS) Code	14
Interest and Penalty Rates	15
Initial Tax Rating Process	16
Tax Rate Changes	17
Additional Configurations and Business Processes Needed to Increase Data Integrity...	18
Unemployment Insurance Quarterly Reports (UI5) Review.....	18
STAARS Has Both Strengths and Weaknesses Relating to Maintaining Data Integrity	20
Review of Key Data Elements in STAARS.....	20
Improved Validations and Processes Would Help Ensure Data Integrity.....	23
Protecting STAARS Data Used in Employer Audits	24
System Documentation.....	25
CHAPTER IV – CHANGE CONTROL	27
Introduction	27
Change Control System Needs Improved Access Management.....	27
Authorized Migrations and Segregation of Duties Issues Identified.....	28
Change Control Documentation Requires More Detail.....	29
Change Control Monitoring Improvements	30
DEPARTMENT RESPONSE	
Department of Labor and Industry	A-1

FIGURES AND TABLES

Figures

Figure 1	STAARS Users	2
Figure 2	STAARS Data Entry Methods	12
Figure 3	Employer Filing Methods in 2015.....	13
Figure 4	Issue Prioritization for Unemployment Insurance Division Systems	31

Tables

Table 1	STAARS Segregated Processes.....	9
Table 2	Social Security Number Verification Sample Results	22

APPOINTED AND ADMINISTRATIVE OFFICIALS

Department of Labor and Industry

Pam Bucy, Commissioner

Galen Hollenbaugh, Deputy Commissioner

Brenda Nordlund, Administrator, Unemployment Insurance Division

George Parisot, Chief Information Officer

Sandy Bay, Chief, Unemployment Insurance Contributions Bureau



MONTANA LEGISLATIVE AUDIT DIVISION

INFORMATION SYSTEMS AUDIT

Data Integrity of the Status, Tax Accounting, Audit, and Rating System (STAARS)

Department of Labor and Industry

SEPTEMBER 2016

16DP-01

REPORT SUMMARY

In 2015, STAARS processed an average of more than 500,000 employee wage records every quarter totaling approximately \$140 million taxes paid by employers for the year. One-third of that information is still gathered through manual input. Considering the large amount of manual data entry, the department has made efforts to ensure data errors are minimized. However, improvements can be made in access management, data validations, and system changes to increase data reliability, accuracy, and completeness.

Context

The Unemployment Insurance (UI) Contributions Bureau of the Department of Labor and Industry (department) relies on STAARS to manage program operations including:

- ◆ Employer registration, status determination, and rating
- ◆ Quarterly reporting and tax payments
- ◆ Collections and refunds
- ◆ Employer auditing

STAARS was implemented in spring of 2014 to replace an unstable and outdated mainframe system. Benefits include workflow management, documentation management, and improved process management.

The system stores personal information for reported employees in Montana throughout the year. This information is used by various divisions for labor statistics, wage verifications, and other metrics involved in determining UI tax rating. One-third of this employee information is manually entered in to the system. Due to the inherent risk of manual

data entry and unemployment insurance fraud, this audit focused on the integrity of data within STAARS. The process for changing or updating the system was also reviewed. Without increased data integrity and control over system changes, the department is at risk of unauthorized changes, incorrect data, and data manipulation reducing the reliability and usability of the data.

Results

Audit work included review of data within the system and verification of current data validations used by the department. Our work identified both erroneous data values and numerous blank data values within STAARS. While errors are expected due to the high amount of manual entry of data, improvements can be made to prevent as much of this type of data from being entered in to STAARS as possible, including validations of data at point of entry and verifications that can be done after data has been entered.

The review of user access identified users with excess privileges and full access to processes that otherwise required two users to be

(continued on back)

involved. While necessary, these forms of privileged access are not actively monitored by the department. No documentation of access management procedures specific to STAARS exists and there is no process to review user access periodically or after a period of inactivity. Improvements will reduce the risk of unauthorized access and system misuse, as well as align with department policy.

While the department has a change control process that is managed through a system that is integrated with STAARS, certain enhancements will improve the security of the process. Documentation excluded details of the entire process and how policy is implemented, access to the change control system is not formally managed, and process improvements need to be made in monitoring for effectiveness and ensuring authorized code is migrated to production according to department policy.

Recommendation Concurrence	
Concur	9
Partially Concur	2
Do Not Concur	0
Source: Agency audit response included in final report.	

For a complete copy of the report (16DP-01) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to lad@mt.gov; or check the web site at <http://leg.mt.gov/audit>
 Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
 Call toll-free 1-800-222-4446, or e-mail ladhotline@mt.gov.

Chapter I – Introduction and Background

Introduction

The Status, Tax Accounting, Auditing, and Rating System (STAARS) is managed by the Unemployment Insurance Division (UID) of the Department of Labor and Industry (department) and directly supports the business functions of the Unemployment Insurance Contributions Bureau within UID. STAARS is used to manage all unemployment insurance (UI) tax administration and provides self-service capabilities for Montana employers. This includes gathering employer paid wages, calculating taxes based on taxable wages and tax rates, and collection of those taxes. Various other account activities involved in this process are also managed through STAARS, such as payment plans and collection activities, general account management, and refunds. STAARS is also used in the employer audit process and to provide information for federal audits of the program.

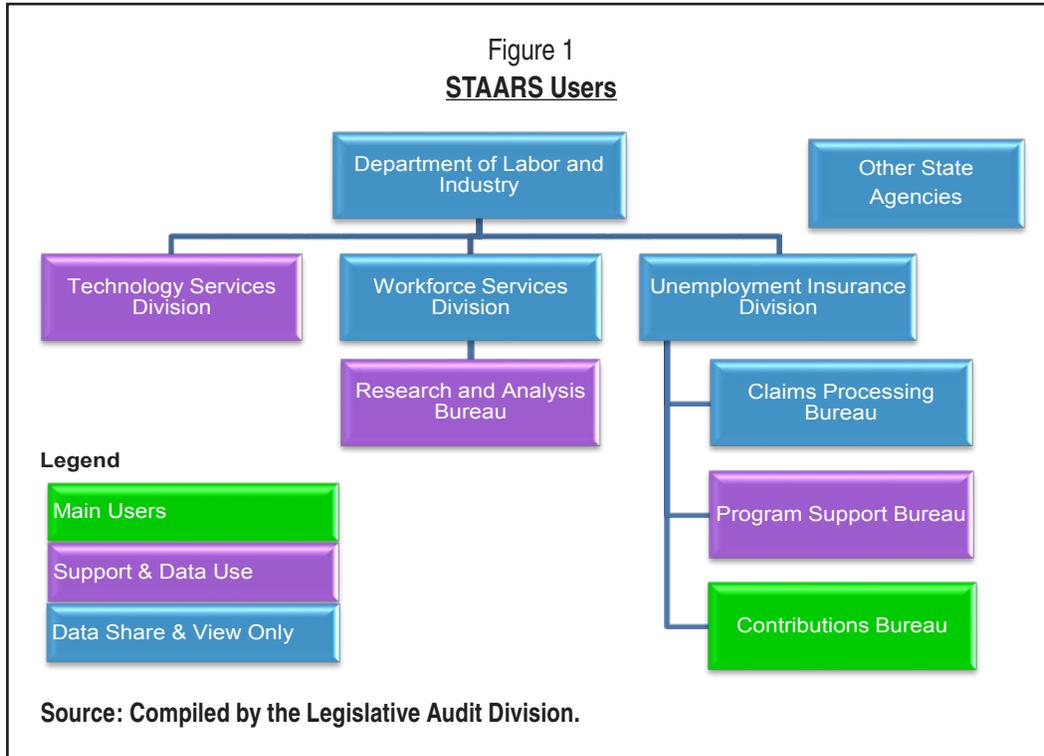
Background

STAARS was implemented in spring 2014 to replace an older, unsustainable system and to provide the following improvements:

- ◆ A self-service web portal for employers
- ◆ Workflow and document management
- ◆ Automated reporting
- ◆ Improved security with the addition of new user roles and functions
- ◆ Integration between UI tax and UI Claims system

STAARS is a commercial, off-the-shelf system that cost \$12.5 million and has been configured to support unemployment contributions for Montana. After the implementation in early 2014, the contractor still assisted with the majority of STAARS management through the warranty phase, which ended May 2015. The department is currently in a maintenance phase with the contractor for roughly \$1 million this year with slight increases each year until 2023. The contractor has dedicated staff working on-site at the department to assist in enhancement development and system issues that cannot be addressed by department staff.

STAARS manages the basic work flows of the UI Contribution Bureau and shares data with other bureaus for their operations. Users of the system are shown in Figure 1 (see page 2).



The UI Contributions Bureau manages the main functions supported by STAARS. Other bureaus and divisions also support or use STAARS in different capacities, including the Research and Analysis Bureau for labor statistics and industry information, the UI Program Support Bureau for user management processes, and the Technology Services Division (TSD) for technical support. External users in other state agencies also rely on shared data from STAARS.

Audit Scope and Objectives

There are multiple systems used in managing the Unemployment Insurance Program within UID. STAARS manages UI tax collections from employers, and maintains data used in assessing these taxes against employers, such as workers' social security numbers and quarterly wages. Due to the information managed by STAARS and the need for complete data to ensure the accuracy of unemployment taxes and other programs that use this information, data integrity was the focus of the audit. A separate system, MISTICS, is used for unemployment insurance claims and was not within the scope of this audit.

Objectives for the audit were:

1. Determine if processes exist in the following areas to ensure data integrity:
 - a. Access management

- b. Manual input and adjustment of data
 - c. Data validations
2. Determine if a process is in place to ensure security and effectiveness of change control.

Methodology

Methodology for this audit included:

Interviews: Discussion with various users and managers of the system including users from the Contributions Bureau, Research and Analysis Division, TSD, and Program Support Bureau.

System testing and observation: Observed daily tasks of staff while working in the system. System validations and processes were also tested and reviewed in the test environment of STAARS.

Data review: Various tests were done on data from 2015 that is stored in the system including:

- ◆ Employer information: Business Name, Federal Employer Identification Number (FEIN), UI Account ID
- ◆ Report information: Gross Wages, Excess Wages, Taxable Wages, Tax Due, Total Rate, and Filing Period
- ◆ Employee Information: First Name, Last Name, Employee Wages for the quarter, and Social Security Number (SSN)

Comparison to Industry Standards: We compared various processes to industry standards. Industry standards used include:

- ◆ Control Objectives for Information and Related Technology (COBIT): Standards for Information Technology (IT) management and governance. These standards outline control practices to reduce technical issues and business risks.
- ◆ National Institute of Standards and Technology (NIST): Provides a catalog of security and privacy controls for information systems. Montana state policy requires the use of NIST as guidance for security risk management and has established baseline security controls from NIST.
- ◆ Internal TSD policies and standards.

Overall Summary and Report Organization

Current configurations within STAARS and business processes minimize the amount of data errors considering that a large portion of the data within the system is manually entered. However, there are improvements that can be made in regard to access

management, data validations, and system changes to increase data accuracy and completeness. This report addresses findings in the following chapters:

- ◆ Chapter II – User Access Management
- ◆ Chapter III – Data Integrity Review
- ◆ Chapter IV – Change Control

Chapter II – User Access Management

Introduction

Access management is the process of granting authorized users the right to specific system functionality, while preventing access to non-authorized users. This process involves documenting approved access, assigning access based on business needs, and regularly reviewing system access rights of users. This maintains data integrity by ensuring the system and data are not being misused or altered by unauthorized users.

Without proper access management, data integrity can be compromised and there is an increased risk of inappropriate system use. Specific to STAARS, users with inappropriate or unmanaged access could adjust critical information, such as wages, Social Security Numbers (SSNs), employer tax rates, or other reporting and employer information. Through the review of user access management, processes that need to be improved or implemented were identified in the access management process, documentation, and monitoring.

Improving Documentation and Defining Responsibility for the Access Management Process

The access management process encompasses the procedures to grant, review, and terminate system access. Industry standards require access be reviewed periodically, unnecessary access be removed immediately, and that documentation of these procedures exist. The Department of Labor and Industry's (department) internal policies also require that these procedures be documented and implemented. These procedures should be documented and detailed enough to ensure consistency and proper handling of access management. Without consistent procedures, unauthorized access is more likely to occur.

To review the access management process, a sample of users was taken to identify proper documentation of authorized access. The process to grant access within the division is standard, including the manager filling out a form noting the user, the systems that require access, an employee signature noting understanding of the confidentiality of information, and supervisor signature to authorize access. This form is then sent to the security officer to establish an account for the user.

Access Documentation Problems Were Identified for the Majority of Users Sampled

Sixty-nine STAARS users were reviewed: 63 randomly selected and six additional users judgmentally chosen due to their heightened privileges or known termination.

We identified 51 users (74 percent) that did not have access forms, meaning there was no documentation authorizing their access to the system. For the remaining 18 users, forms were identified but had the following issues:

- ◆ Fourteen forms did not document the role or necessary access for the user.
- ◆ Thirteen forms were missing information including:
 - ◇ Six user signatures were not obtained prior to access being granted,
 - ◇ Seven users requested access to MISTICS, the UI claims system, not STAARS, and
 - ◇ One termination form was missing a supervisor's signature.

During this review, no procedural document was identified outlining the security officer's role to manage access or the processes for granting, reviewing, or terminating access. There is policy in place for access management; however, there is not a process specific to STAARS outlining how policy is enforced or who is responsible for the process. The lack of standards for the procedure lead to inconsistent processes being followed to provide a user access to the system. We identified that when the new system was created, users were not required to fill out a form identifying their requests or necessity for system access.

Periodic Monitoring of System Access Is Not Occurring

Audit work also identified the department is not periodically reviewing user access or user inactivity. Since there is no review by the department, audit staff reviewed users who had no system activity for a year. Fifty-eight inactive users were identified. Of the inactive users, one user had been terminated and removed from the system since the user list was created and the other is the division administrator with view only access. The access for the majority of the remaining 56 users is view only; however, STAARS contains personal and confidential information that should be protected from users that do not need to access the system. Three of the 56 users were developers with access to update or change system configurations. One of the users with developer access left the project in September 2015 and had not been removed from the system when access was reviewed in May 2016.

The department has standards requiring inactive users be locked out of Active Directory after 45 days of inactivity, but this process is not specific to STAARS. Active Directory manages state employee access to the state network. A user could be active in Active Directory while being inactive in STAARS and the STAARS account will not be deactivated. The department indicated it has started working with the contractor to include a STAARS specific deactivation process in the next system upgrade.

While the department has a structure for access management and policies to be followed, the responsibility of this process has changed since the system was implemented and created the opportunity for inconsistent processes to be used. A clearly defined and documented process needs to be developed to ensure appropriate access to STAARS. Additionally, clearly defining procedures and roles and responsibilities for managing access will ensure consistency in how policy is enforced. Reviewing user access and terminating inactive users periodically will also reduce the risk of unauthorized access.

RECOMMENDATION #1

We recommend the Department of Labor and Industry:

- A. *Establish and document procedures for granting, reviewing, changing, and terminating access, and*
 - B. *Define roles and responsibilities of staff involved in access management and document them within procedures.*
-

Improvements Needed in Defining and Monitoring User Access Roles and Privileges

Individual user access was reviewed to ensure the least amount of privilege necessary was granted and that segregation of duties exists so no single user can circumvent a critical process in the system. These controls are included in the department's Technology Services Division's (TSD) access standards. They are further defined in information systems industry standards to prevent unauthorized access and reduce the risk of system manipulation or misuse.

During audit work, 173 executable actions in the system, known as functions, were identified. Users are generally assigned to a group of like functions through defined user roles when access is granted to improve efficiency and consistency. Our review was hindered due to there being no documentation to clarify what each of the 173 functions allows a user to do within the system. Short descriptions were available, but required further clarification by department staff in some cases. With the descriptions that were available, a review was still possible, but was limited in nature due to the lack of clarification of roles. TSD standards also include account management practices that define group and role membership and specify access privileges to make clear what an individual can access when assigned certain privileges.

Over-Assigned User Privileges Exist

To review user privileges the following tests were completed:

- ◆ Comparison of Contributions Bureau staff user roles and appropriateness to their work responsibilities.
- ◆ Identifying Contribution Bureau staff roles assigned to users not working in the bureau.
- ◆ Staff interviews to understand what interaction was needed to perform job duties and compared to system access.

Through these reviews, instances of excess access were identified including three users outside of the Collections Bureau who had bureau access. Details include:

- ◆ Functions assigned to groups that were excessive and unnecessary.
 - ◇ Security officers allowed to change industry codes.
 - ◇ Security officers allowed to edit penalty rates.
 - ◇ Editing employer information beyond the necessary classification code allowed to research and analysis group.
- ◆ Two users with inappropriate access due to access being copied from the previous person who held the position without further review for appropriateness.
 - ◇ Rating/Status business analyst with ability to change penalty rates in the system.
 - ◇ TSD business analyst with registration access.

We also identified staff with more access than needed for their roles. For example, we found three users were provided access to approve employer audits although this is not part of their job duties. Department staff agreed the functions were not necessary for the groups they were assigned to and will review and update the assignments. With the number of functions and groups within the system, a periodic review for appropriateness of user roles and functions assigned to user groups is necessary.

These issues increase the risk of fraud and system information changes, whether intentional or not, by a user who is not authorized or possibly untrained in the excess functions. Creating role and function documentation will clearly define the least privilege allowed for each user of the system and assist in enforcing TSD policy. Updating this information as business processes and the system change will ensure access issues are not created due to changes. This will reduce the risk of unauthorized access and increase data integrity related to the system.

RECOMMENDATION #2

We recommend the Department of Labor and Industry:

- A. *Clearly define and document the activities the user is allowed to carry out based on the function and which function or role each position should have.*
- B. *Review the functions assigned to each group on a periodic basis to ensure appropriateness as business processes and system changes occur.*

Monitoring of Privileged Users Should Occur

Functions that are part of a process requiring involvement of more than one user, such as create and approve functions, were reviewed to ensure no user had access to both functions at the same time. Segregation of duties within certain processes is necessary to ensure accuracy and reduce any specific risks associated with the process.

Specific segregations are currently not documented to identify which functions should not be allowed to certain users due to their job descriptions or due to their access to other functions. For example, there is no documentation stating the need for the function to add refunds and the function to approve refunds be separated. Without this documentation, a review of system functions was necessary to identify pairs of functions that should be segregated. However, more function pairs could exist than those identified in Table 1.

Table 1
STAARS Segregated Processes

Initial Function	Secondary Function	A user with both can . . .
Add Account Adjustments	Approve Account Adjustments	Create and approve adjustments and suspend or write-off debts
Add Account Appeal	Approve Account Appeal	Create and approve the same appeal
Submit Audit	Approve Audit	Approve his/her own audit
Add a Payment Agreement	Approve a Payment Agreement	Approve his/her own Payment Agreement
Add Refund	Approve Refund	Approve his/her own refund
Add/Amend Employer Reports	Manage Collections	Adjust reports to affect collections

Source: Compiled by the Legislative Audit Division.

This table shows the pairs of functions identified by audit staff that are segregated within the system. For example, a user assigned access to both create and approve a refund can approve refunds he/she created without the review or approval of another person. With access to both of these types of functions, a user could potentially commit fraud on their own or the behalf of an employer.

Our review of segregation of duties identified the following concerns:

- ◆ Two users with the ability to add and approve adjustments.
- ◆ Four users with the ability to add and approve refunds.
- ◆ Five users with the ability to add and approve audits.
- ◆ Four users with the ability to amend employer reports and manage collections.
- ◆ Three users with the ability to add and approve payment agreements.
- ◆ Three users with the ability to add and approve appeals.

The department reviewed these findings and determined access can be adjusted within the refund process to limit anyone from access to create and approve refunds. Access to approve audits will also be adjusted once a new audit manager is hired because the lack of segregation was due to back-up needs. Access to add and approve adjustments is limited to only the supervisor and direct back-up. The department stated the remaining processes did not have enough risk associated to warrant limiting access and are used for back-up reasons. The department also pointed out audit trails and reports within the system that track everything a user does. However, the department stated that certain reports are only reviewed twice a year for staff's performance evaluation purposes, but not for all of the privileged functions or segregated duties.

While we understand that it is sometimes necessary for users to have excess access for back-up reasons, these functions are not part of daily business needs and are considered privileged. These privileged functions should be consistently monitored to ensure they are not being taken advantage of or misused, especially if segregation cannot be maintained or if the function is privileged.

RECOMMENDATION #3

We recommend the Department of Labor and Industry:

- A. *Create documentation of and enforce segregated processes within the system, and*
 - B. *Implement a process to monitor privileged functions including areas where segregation cannot be maintained and users have access beyond their business need.*
-

CHAPTER III – Data Integrity Review

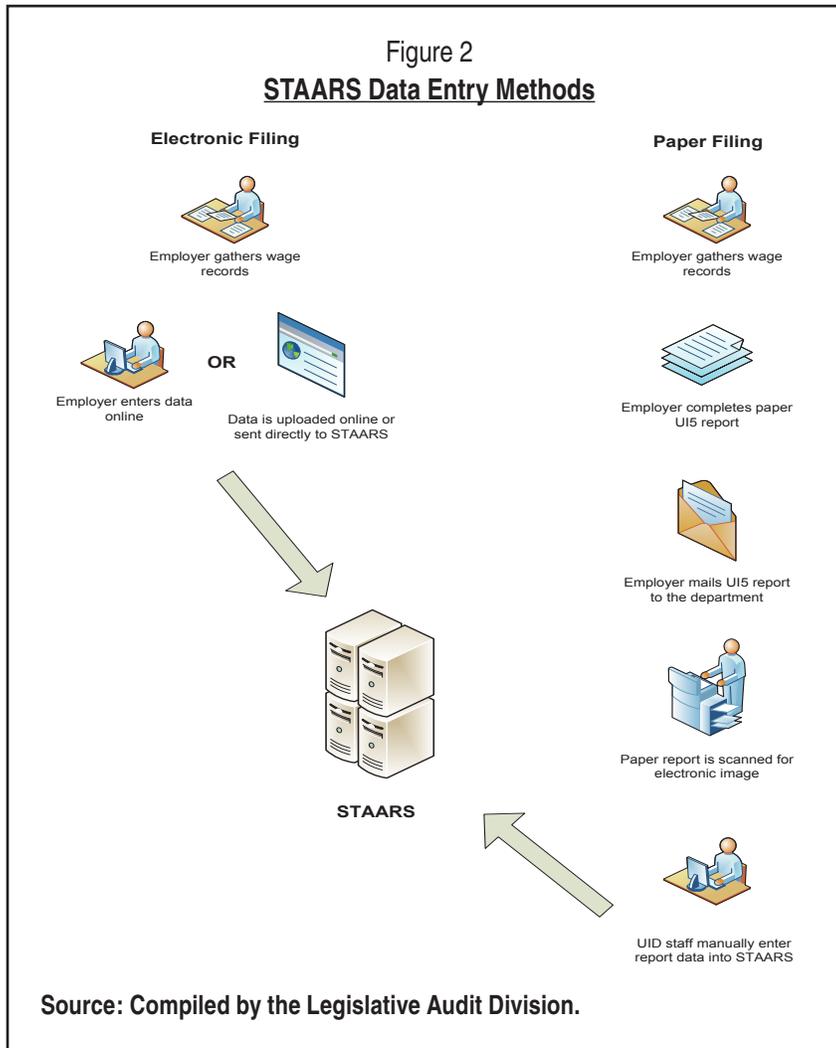
Introduction

Data integrity refers to completeness and accuracy of data. Managing data integrity ensures that:

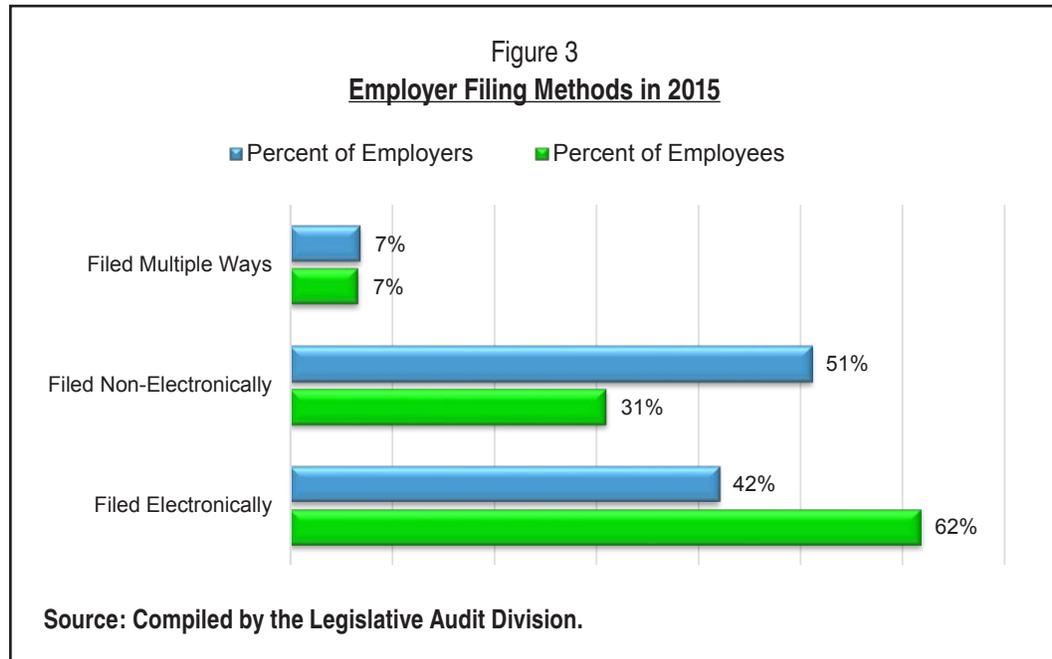
- ◆ Unemployment taxes are calculated accurately and therefore paid appropriately.
- ◆ Unemployment claims are issued accurately.
- ◆ Data used in calculating labor statistics is accurate and therefore factors such as average weekly wage and unemployment insurance amounts are accurate.
- ◆ Data used in calculating federal statistics is accurate.
- ◆ Data shared to assist in fraud detection within other agencies and systems is accurate and useful.

Without effective validations, incorrect data would be allowed in the system and could impact the accurate management of Unemployment Insurance (UI) accounts within the state and ultimately affect the data shared with partners that rely on this data for their operations.

The main function of the Status, Tax Accounting, Audit, and Rating System (STAARS) is to manage quarterly UI reports from employers. This involves receiving the majority of data used and stored by STAARS, including employer calculated wages and taxes and individual employee wage information. This data can be received electronically or manually entered if an employer sends in a hard copy report, as shown in Figure 2 (see page 12). A major risk to data integrity is manually entered data. Other risks specific to STAARS also exist, such as reporting errors committed by the employer, intentional or not.



Approximately 42 percent of employers are reporting electronically every quarter. These employers are collectively reporting data for approximately two-thirds of Montana employees whose data is maintained in STAARS. However, over half of reports filed are paper reports that need to be manually entered by Department of Labor and Industry (department) staff every quarter, representing roughly 31 percent of all employees reported. In the 2015 Legislative Session, SB105 included revisions to current law that would have required large employers to file electronically. However, the bill was amended and these revisions were removed from the bill before it was passed. Figure 3 (see page 13) illustrates the percentage of employers and employees that are reported electronically and through hard copy paper reports.



Due to the high amount of manually entered data into the system and inherent risk of UI, system and manual processes that maintained data integrity were reviewed. This included identifying processes for how data is manually entered and how data can be adjusted by users. System configurations and manual business processes that ensure this data is accurate were reviewed. Once there was an understanding of what safeguards existed and possible weaknesses, tests were designed to review all of the reported data within the system.

The following sections discuss the processes reviewed, results of data tests conducted, and where improvements can be made to ensure better data accuracy and completeness.

Manual Data Input and Adjustments

Manual data input and data adjustment safeguards are important to maintaining control of business processes and increasing data integrity. Such controls are crucial to STAARS with the amount of wages in the system that are entered manually as opposed to electronically. Accuracy and completeness cannot be completely assured for any system where manual entry is prevalent, but safeguards can be put into place to significantly reduce errors. Business processes ensure that information related to and processed by the system is accurate and complete to the satisfaction of the department and data-sharing partners. These processes include:

- ◆ System controls: Internal system settings or configurations to enforce a safeguard.
- ◆ Manual controls: Processes outside of the system enforced by the user.

Certain processes or fields within the system were reviewed for system or manual controls that would increase data integrity. Three areas of controls were reviewed for each process or field:

- ◆ **Input Controls:** Controls at the time the data is entered in to the system that include field validations or restrictions to ensure the data entered is as close to accurate and complete as possible.
- ◆ **System Validations:** Systematic controls after the data is entered in the system that include address verifications or system forced approvals/reviews.
- ◆ **Approval/Review Controls:** Manual processes completed by the user after the data is entered in the system that include approvals or report reviews that are not forced by the system.

The following sections discuss the areas reviewed and specific concerns relating to industry classification codes, interest and penalty rates, tax rates, and tax rate changes.

North American Industry Classification System (NAICS) Code

The NAICS code is a description of the employer that identifies its industry. This code is used to determine the rating scale and individual tax rate for new employers, in federal reporting, and in research and analysis of employment within Montana. Because of the importance and significance of these industry classifications, department staff in the Research and Analysis Bureau (R&A) specialize in determining NAICS codes.

Within STAARS, the NAICS code is entered at the time of registration and then pulled into the tax rating process for new employers. However, the processes for registering an employer's NAICS code and for applying the code during tax rating are separately managed within STAARS, so one can be changed without updating the other. Due to this, system validations and processes relative to each NAICS code used for registration and tax rating were reviewed and the following was identified:

- ◆ A registration user can approve an employer registration without the NAICS code being reviewed by the appropriate staff in R&A.
- ◆ Since both registration and R&A users are updating NAICS codes and the system does not require a reason or notes for these changes, communication and documentation of when changes are made need to be improved.
- ◆ The NAICS code field that is part of the rating process does not have the same input validations as the NAICS code in registration, so the NAICS code can be changed to an invalid code.

Interest and Penalty Rates

When an employer fails to pay taxes in a timely manner, a collection process begins to obtain the taxes with penalties and interest. These are established in §39-51-1301, MCA; however, through the collection process, penalties and interest can be partially or totally waived. According to the department, this is done to conserve the relationship with the employer and encourage the employer to pay taxes more consistently. These changes are referred to as abatements and custom rates.

The collection process usually starts with the establishment of a payment agreement with the employer if the employer cannot pay the amount in full. Payment agreements consist of monthly payments toward past due amounts as well as timely payments of upcoming quarterly taxes. Most abatements and custom rate changes occur as part of these payment agreements, but can be done without an agreement.

Due to the importance of the assessment of interest and penalties, strong control over the process to change them is necessary to ensure they are done accurately. Current system configurations that assist in the process include:

- ◆ Only authorized collections staff can abate penalties and interest or establish a custom interest rate.
- ◆ Only authorized collections staff can establish payment agreements.
- ◆ Payment agreements that are longer than three years or less than \$50 a month require approval.
- ◆ Abatements established without a payment agreement require supervisor approval within the system.
- ◆ When establishing an abatement, the type of abatement and notes are required. If the abatement type is not part of a payment agreement a reason is also required.

While these configurations reduce some risk, there are areas identified where vulnerabilities still exist. Audit work identified that custom interest rates do not require approval and payment agreement abatements can be selected without an agreement actually being created, therefore bypassing any required approval. Since the system forced approval can be bypassed, another control should be added to verify the payment agreement exists so the abatement is ultimately approved. This approval process ensures collection staff are accurately and consistently establishing abatements.

When trying to identify additional business processes for these two occurrences, the department noted a system report that identifies all payment agreement adjustments, including any abatements or custom rates. This report is used twice a year for employee

evaluations to review employee activity, not as a manual process for reviewing or approving payment agreement abatements to ensure that an agreement was established.

The department also noted that with the number of changes made, it would be inefficient to review all of them. While reviewing all changes would be a high level security, this needs to be balanced with efficiency. Setting a threshold for higher-risk changes or establishing a consistent review of a portion of the changes are controls that would also increase accuracy of data.

Initial Tax Rating Process

Through a lengthy process, employer rates are established annually for the upcoming year. Employers are categorized in two ways for UI tax rating purposes: reimbursable and experience rated. Reimbursable accounts do not pay taxes and only nonprofit or governmental employers meeting certain criteria are eligible. Of the employers who are experience rated, four different rating processes occur based on the type of employer.

Experience Rated: Private and for-profit employers that have been reporting wages and paying unemployment taxes for three years or more.

Industry Rated: New private and for-profit employers with less than three years of experience paying unemployment taxes.

Governmental Experience Rated: State and local government employers that chose to be experience rated or do not qualify to be a reimbursable account.

New Government Experience Rated: Governmental employers that do not have three years of history.

All of the processes follow the same general path. A matrix of rates and employer class boundaries is identified based on the last year's performance of the same type of employers. The matrix of rates for each type is established in law and in rule, and the boundaries for the classes in the matrix are established by department staff to ensure that the Unemployment Insurance fund will end the next year as close to the required level as possible (governmental employers boundaries are predetermined in their matrix). The class is determined by the reserve ratio for experience rated employers and the benefit ratio for governmental employers.

Spreadsheets and STAARS reports are used to determine the class boundaries for experience rated employers. Once determined, these boundaries, the median rate, and the average rates for industry rated employers are entered in to tables within the

system through the change control process. The system then uses the previous years' contributions, benefit charges, and wage totals to calculate the reserve ratio and benefit ratio. The UI tax rate is then determined based on the updated matrix of rates and the calculated ratio.

CONCLUSION

The department ensures initial accurate employer UI tax rates by updating metrics systematically through the change control process and conducting manual tax rate verification after each rating process.

Tax Rate Changes

Rates are calculated once a year, or when a new employer is registered, and should not change throughout the year unless the rate is appealed, the rate is transferred to a new employer, changes were made to the numbers used to calculate the reserve ratio, or updated information is received within 30 days of registration. Of these changes, the only ones that are manually done are when updated information is received within 30 days of registration or when changes are made to the numbers used to calculate the reserve ratio: contribution total, wage totals, or benefits charged total. The other changes to tax rates are completed by the system automatically when other events happen, such as an experience transfer.

The system controls changes to tax rates by:

- ◆ Not allowing users to directly change the rate, only the numbers used to calculate the rate.
- ◆ Requiring a reason and note for every change on the rating screen.
- ◆ Documenting who made the change and at what time.
- ◆ Keeping an audit trail of the previous rating calculations for comparison after changes are made.

These configurations reduce the risk of incorrect rates, however, users with access to change rates can adjust the numbers or NAICS code used to calculate rates without any approval or review of the rate changes. Users with this access include the rating specialist and two registration employees who are not directly involved with the rating process.

The system requires a reason and notes when these changes are made and has various reasons for the user has to choose from for the change, including "other." However, the report identifying these changes does not list reasons for the changes. According

to the rate change report in the system, 503 changes to individual employer rates have occurred since STAARS was implemented. This is a small number compared to the 40,000 employer accounts managed by the system. Due to the minimal reasons for manual changes after rates have been established, changes not done systematically should have increased safeguards, such as verification or periodic review. This will ensure that changes made are appropriate and if not, are caught in a timely manner to protect the department and employers.

Additional Configurations and Business Processes Needed to Increase Data Integrity

Through review of system configurations and business process, specific fields where validations can be increased and processes that can be improved were identified including:

- ◆ NAICS code validations on the rating screen.
- ◆ NAICS code review and change communication and documentation.
- ◆ Custom interest rates do not require approval.
- ◆ Payment agreement abatements can be selected without an agreement being created.
- ◆ Tax rate changes are not approved or reviewed.

The system tracks user activity and has reports available for some of these concerns; however, a process to review these reports and user activity consistently needs to be established to better utilize them. Increased thresholds for when the system triggers approvals for certain events can also increase these controls. These improvements will decrease data integrity risks and errors in data used in labor statistics and shared with other systems.

RECOMMENDATION #4

We recommend the Department of Labor and Industry increase systematic and manual controls related to NAICS code, custom interest rates, payment agreement abatements, and tax rate changes.

Unemployment Insurance Quarterly Reports (UI5) Review

Manual data input and adjustment audit work included a review of the Unemployment Insurance Quarterly Reports (UI5) process because this is where the majority of data in STAARS enters the system. The findings from this review were used to identify tests

that should be conducted on 2015 wage report data. Once the tests were identified, the data from 2015 was reviewed for data errors.

In the UI5 process, invalid data can occur for different reasons, including department staff data entry error, employer reporting error, or intentional fraud. Strong, documented controls reduce inaccurate data by ensuring consistent validation for all manual or electronically entered data, outlining system response to invalid data, and defining the process for consistent invalid data remediation.

At the end of every quarter, employers have one month to provide their UI5 reports that detail gross wages paid, wages paid that are over the excess wage limit for the year, tax rate, taxes due, and number of employees employed on the 12th of each month in the quarter. These reports also provide individual employee information including name, SSN, and wage information.

Currently, 32 percent of employees reported are manually entered. Through discussion with staff responsible for entering this information and entering reports manually in the test environment, the following controls were identified:

- ◆ Social Security Number (SSN) cannot have alphabetic characters and must be 9 digits.
- ◆ Wage fields cannot have alphabetic characters.
- ◆ The system compares the total of individual wages entered to the total wages reported by the employer and will provide a warning to the user trying to process the report where an error is identified.
- ◆ The report can be saved with the errors, but the report status will be in error until the sum of individual wages entered matches the total wage numbers reported or the report is flagged as being unbalanced and accepted.
- ◆ The system forces action on variances over \$100.

When testing report entry, the following observations regarding increased risk of data errors were also made:

- ◆ SSN can be left blank and duplicate SSN can be entered.
 - ◇ The system identifies these, but the report can still be processed and the issue can be overridden.
 - ◇ The system automatically sends a letter informing the employer that the SSN issue needs to be addressed.
- ◆ There is no verification for SSNs.
- ◆ First name of employee is not required.
- ◆ It is standard operating procedure to enter only the last name of employees when manually entering reports.

- ◆ First and last name can have any type of character entered, including alphanumeric and symbols.

STAARS Has Both Strengths and Weaknesses Relating to Maintaining Data Integrity

The observations noted above show that STAARS has both strengths and weaknesses relating to maintaining the integrity of data for the UI5 reporting process. Based on these observations, further testing and analysis was conducted and opportunities were identified for the department to make improvements in the following two areas:

- ◆ Improving validation process for specific data elements, including SSNs, employee names, and NAICS codes.
- ◆ Upgrading security measures where UI5 data is used during field audit activities.

The following sections discuss these two issues.

Review of Key Data Elements in STAARS

STAARS data was reviewed to test the system configurations for validating key elements. The department provided reports that totaled over 2 million wage records for 2015, including over half a million employee wages recorded for each quarter. The reports included the following information:

Employer Information: Business Name, Federal Employer Identification Number (FEIN), UI Account ID.

Report Information: Gross Wages, Excess Wages, Taxable Wages, Tax Due, Total Rate, and Filing Period.

Employee Information: First Name, Last Name, Employee Wages for the quarter, and Social Security Number (SSN).

Based on information provided from the UI5 report process review, the following audit tests were conducted:

Wage Differences: The sum of individual wages was compared to the total gross wages based on the report provided. The system identifies when these two numbers do not match; however, the report can still be processed and “pushed through.”

The review found 563 reports that did not match; however, only 81 had a discrepancy of more than \$100. The department does not follow up on differences under \$100. The reports with differences under \$100 totaled \$893.05. Only six reports that were

reviewed were unresolved, totaling \$156,117. The system identifies any reports that show a wage difference and creates a work item to be reviewed. If there is no entry issue found, the employer is then contacted about the discrepancy. The department noted that the correct procedure is for three attempts to contact the employer be made, but in the system, only one phone call was documented on the unresolved reports identified. Without documentation, it is unknown if all attempts were made to contact employers and correct the reports.

Blank Data: Blank employer information, employee information, and SSN were reviewed. STAARS generated a report that was used to identify blank SSNs. Blank data was expected in the name fields, so this test was run to identify how much of the data is blank and whether the data was from electronic filing or manually entry.

Almost 700,000 records of the 2 million reviewed were identified with either employee first or last name missing. There were 235 records identified that were missing last name. When looking at the data entry method for blank data, the majority of issues came from manually entered reports and all records missing last name were from manually entered data.

The specific report in the system that identifies blank SSNs was reviewed. The report identified 271 blank SSNs in 2015 data. When a SSN is not reported, the system identifies the blank SSN and sends a letter to the employer as soon as the report is processed. If the SSN is not fixed in 15 days, a warning in the system is created and the employer is contacted. If the SSN is not fixed in 30 days, a second letter is sent and the employer is contacted again. If these attempts are unsuccessful, the blank SSN is accepted and the error message is overridden in the report. Without a SSN for the employee reported, the reported employee is not verified and tax calculations could be affected later in the year for the employer.

SSN Verification: Two different tests were done to identify potentially incorrect SSNs within the department's data.

- ◆ **Duplicate SSNs with Different Names:** Duplicate SSNs were expected due to employees with multiple jobs and working in multiple quarters throughout the year. However, the names reported with those SSNs should be the same, or at least similar.
- ◆ **Last Name Comparison to Tax Information:** The Department of Revenue (DOR) provided information that included first and last name and SSN. This report was then matched to the department reports by SSN and the last names were compared.

Multiple reasons could lead to the names not matching for both tests, so a sample of records was reviewed individually from each test. Issues identified were instances where the name clearly did not match and there was not enough information available to justify the difference, such as a name change. These tests identified some of the errors, but without complete names stored in the system, all errors could not be identified.

Both tests identified SSNs which appeared to be incorrect. Table 2 shows the categories determined by audit staff used to describe the reason for the last names not matching: last names that were clearly different, last names that were different due to apparent name change, and names that were different due to a data inconsistency like misspelling, spacing differences, or inconsistent use of a suffix. Between 6 and 10 percent of the SSNs in the samples could be potentially fraudulent based on the results.

Table 2
Social Security Number Verification Sample Results

SSN Classification	Department of Revenue Data Comparison		Duplicate SSN with Different Name	
Different Last Name	83	10%	45	6%
Inconsistent Data	653	78%	605	78%
Name Change	104	12%	121	16%
Total Sample	840		771	

Source: Compiled by the Legislative Audit Division.

Invalid SSN: According to the Social Security Administration, there are certain characteristics that a valid SSN cannot have and there are SSNs that could be valid, but are more likely to be used in fraud or to be a data entry error. The wage list provided by the department was reviewed for these characteristics. Searches for known, invalid SSNs identified 258 SSNs reported in 2015 wage reports and 1 SSN that was unlikely valid.

Differing NAICS Codes: The system holds the NAICS code for an employer in two places: the registration screen and the rating screen. For industry rated employers, the NAICS code on the rating screen determines the rate. If this code does not match the NAICS code from the registration tab, the employer could be paying taxes based on an incorrect rate. However, if the employer fails to provide registration information within 30 days of the request for information the rate will not be updated if the information changes the NAICS code.

Two reports from the system were compared: one with NAICS code from the registration tab and one with NAICS classification from the rating tab for industry rated employers. These were compared to see if the code from the registration screen matched the classification on the rating screen at the end of 2015.

This test identified 151 industry rated employers that did not have matching NAICS codes. Each account was reviewed because there are reasons that they should not match, like when the registration information is not received timely. Of the 151 accounts reviewed, 8 accounts were identified as not having a valid reason for having different NAICS codes. This means that the employer paid taxes based on an incorrect rate in 2015, or started 2016 with an incorrect rate. The incorrect taxes totaled \$125 being underpaid by one employer and \$680 being overpaid by the seven other employers in 2015.

These differences occurred because multiple staff are able to change the NAICS code on the registration screen, but some of them cannot change the rate. If a user changes the NAICS code and does not communicate this, the rate will not be updated. Documentation of the change is kept with the account, but there is nothing notifying the users that change the rate about the change to the NAICS code. The system does not identify when these two codes do not match.

Improved Validations and Processes Would Help Ensure Data Integrity

Along with these findings impacting the integrity of STAARS data, they also affect the data provided for labor statistics and shared with other systems in the state. Labor statistics include:

- ◆ Average weekly wage used to set the minimum and maximum weekly wage for unemployment benefits.
- ◆ Taxable wage base set each year.
- ◆ Industry rated employer tax rate schedule.

While the department recognizes changes could be made, due to the amount of time that would be spent on reviewing every record, complete validation is not feasible. Additionally, the department believes the most important data is used in unemployment claims and is verified through MISTICS when a claim is made.

While we do not discredit the department's concern, the department owns the data and data integrity is still important, especially when being used by other sources. Additionally, while reviewing every record would be inefficient for the department,

systematic filters and processes can be created to identify a portion of data inaccuracies and incompleteness. Individual review of these issues may not be feasible at this point; however, there are processes and controls that can be put in place to start identifying some of these data issues on an ongoing basis, including:

- ◆ Systematic filters and processes to identify data inaccuracies and incompleteness.
- ◆ Create criteria for reviewing high risk data error findings instead of every finding.
- ◆ Suggest employers with data error findings for employer audit.
- ◆ Increased system data validations.

With increased and consistent input validations and documented processes to review and resolve issues identified through validations, the department can increase data integrity and the reliability and usefulness of data.

RECOMMENDATION #5

We recommend that the Department of Labor and Industry:

- A. *Increase validation and processes concerning invalid and incorrect SSNs, blank last names, and NAICS codes used in rating, and*
 - B. *Document these validations and the procedures used to remediate any identified errors.*
-

Protecting STAARS Data Used in Employer Audits

During fieldwork, two types of department audits were found that are used to increase data integrity related to employer contributions and their UI5 reports: Tax Performance System (TPS) Audits and Employer Audits.

The TPS audit is federally mandated and conducted by the Program Support Bureau within the department every year to ensure the state is following guidelines and ensuring data quality. When reviewing how the system assists in providing TPS audit information, it was identified that the implementation of STAARS has impacted the ability to complete these audits. The majority of the tests required cannot be conducted because the data needed has not been provided accurately or in a timely manner by the system. These kind of issues are common among other states and USDOL is working with states through corrective action plans to address the issues. In 2016, 50 of 53 states and territories are under corrective action plans, including Montana.

The Unemployment Contributions Bureau audits employers and verifies quarterly reports submitted by the employer. When reviewing employer audits, it was identified that employee data, including SSNs, are pulled from the system and used in spreadsheets to complete the audit. Field representatives travel to various areas of Montana to conduct these audits, so it is necessary to have access to data when the system is not accessible.

Field representatives are directed to save the spreadsheets in a secure drive on their laptops. Currently this secure drive uses encryption software that is not supported. The software is functioning as of now, but if a vulnerability were to be found, there would be no support to fix the issue thus creating a vulnerability to the security of the data. The department has identified this issue and was expected to replace the software in September 2016.

RECOMMENDATION #6

We recommend the Department of Labor and Industry upgrade the encryption software on field representatives' laptops.

System Documentation

Well-defined system documentation and department policies and procedures improve data integrity by defining how data is processed or validated by the system, how the system and department procedures ensure data completeness and accuracy, and how the system and department responds to instances of data errors. System documentation based on industry standards reduces the possibility of system errors going unnoticed, improper use of the system, and assists in identifying inefficient processes.

Throughout the audit, various types of system documentation were necessary to understand how the system should function, how it should be used, and help understand the details of what the system does in various processes. These areas include:

- ◆ Data validations
- ◆ Interface definitions
- ◆ System calculations
- ◆ User access management

The department could not provide detailed system documentation and current policies and procedures relating to STAARS reference the previous system. The department

currently relies on user guides for some specific processes like collections and report functionality, a system manual defining batch processing in the system, the system help function, and change request documentation from the system development process.

The process for configuring the system specifically for the department started with a meeting between the department and contractor showing base system configurations. From there, necessary changes to meet the department's needs were documented as change requests. These change requests plus a few working documents are what the department currently relies on as system documentation.

The department states that full system documentation is not available because the system is proprietary and the contractor will not release proprietary information. State policy adopted by the department requires that documentation for the information system be obtained and protected as required. Within the contract and license agreements with the contractor, it is clearly stated that the system and documentation are the property of the contractor and anything provided by the contractor cannot be shared or duplicated.

If design documents or other procedural documents are not an option due to proprietary nature of the system, a complete system manual or procedural documents should be created that details all processes the system manages or is involved in, what users should expect from the system, and how they should interact with the system. This will improve user understanding of how the system should work and reduce associated risks with improper use.

RECOMMENDATION #7

We recommend the Department of Labor and Industry obtain or develop complete, detailed system documentation that defines:

- A. *Processes managed by the system and how users should interact with the system during these processes, and*
 - B. *How the system is expected to function throughout these processes, including any validations or configurations.*
-

CHAPTER IV – Change Control

Introduction

The evolution of a system includes upgrades, enhancements, issues, and other reasons to change the base configuration of the system. Change control is the process that manages these changes so they all occur according to an established plan and unauthorized changes are prevented. Industry standards require strong controls for the change control process to also ensure it resolves issues efficiently with as little time and cost as possible.

To review security and effectiveness of change control, the change control process was first reviewed for documentation and clarification of exactly what is expected to happen. Once the process was understood, it was then reviewed for the following:

- ◆ Accurate documentation.
- ◆ Only authorized migrations occurred and the ability to approve migrations is separated from the ability to create migrations.
- ◆ Change control monitoring metrics.

Change Control System Needs

Improved Access Management

A separate change control system is used to support the change control process for STAARS. The system tracks all changes, manages change control procedure and flow, and manages daily, automatic migrations of code changes.

This system, just like STAARS, requires users to log in with a username and password and maintains security through user roles and functions. Just like any other system, user access management is important in this system to ensure that changes to STAARS are authorized and the change control system is not being manipulated or misused. The following describes the access management standards we reviewed for access into the change control system and our assessment of these standards.

Documented access requirements (access forms): When users were assigned access in the change control system, there was no formal process for being granted access. The department uses an added note on the STAARS access form if a user needs access to the change control system.

Terminated Users: One user who was terminated at the end of 2015 still had change control access. There was no review process for user access identified.

Privileged Users: Access to migrate code to production or administrative rights were considered privileged. No users were found to have excess privileged access.

Direct Server Changes: Since the change control system does not safeguard against direct changes to code through administrative rights to servers, this access was reviewed. Administrative access to servers is limited to database administrators in the Technology Services Division (TSD). Administrative access is granted to contractors in the change control system; however, contractors do not have this access to servers or to directly change code without the controls within the change control system.

Although we identified several features of the department's change control access process that met the necessary standards, there is still room for improvement. Increased access management, including reviewing access to identify users that no longer need access, terminated users, or access changes for the change control system, is necessary to comply with TSD policy. This will reduce unauthorized access or actions. Documenting and following procedures to manage access to the system are necessary due to the user profiles, roles, and security features of the system. Without these procedures, the security of the system is undermined.

RECOMMENDATION #8

We recommend the Department of Labor and Industry comply with access management policy by documenting and implementing procedures to grant, review, and terminate access to the change control system.

Authorized Migrations and Segregation of Duties Issues Identified

Industry standards and department policy related to access management also require the concept of segregation of duties be followed, as well as limiting privileged access. The privileged access related to the change control system is the ability to approve migrations or code changes from a test environment to production.

When reviewing migrations for authorized user approval, only one migration in the past year had been approved by a user who was not a lead developer, supervisor, or network technician/administrator. This migration was also created by the same person that approved it. This user was a business user, not part of TSD staff. This instance was a table change, and the business process for this specific change has been updated to help ensure this does not occur in the future.

When reviewing system tracking for migrations of code into production, certain issues were identified. Segregation of duties errors where the same person created and approved a migration to production have improved since the system was signed over in May 2015, but there were still five instances found after that date. There were also 62 instances identified where the contractor both created and approved the migration. This poses a risk to the State as no state employee has authorized or reviewed the changes to the system. While some of these changes may be to the proprietary base system, the department should be ensuring these changes do not affect any other system functionality and that the data within STAARS is still secure.

The department relied heavily on the contractor after implementation of STAARS and has since shown improvements in reducing segregation of duty errors. However, there are still occurrences of the issue and further controls need to be implemented to ensure they do not occur again.

RECOMMENDATION #9

We recommend the Department of Labor and Industry develop controls to ensure:

- A. *The person creating the migration is not allowed to also approve the migration, and*
 - B. *Department staff review changes being made by contractors.*
-

Change Control Documentation Requires More Detail

Documentation of change control procedures is important to ensure consistency and authorized changes are made to the system. This documentation should be thorough and, according to industry standards, address roles, responsibilities, and configuration management processes and procedures.

The current change control documentation provided by the department is vague. It includes some roles and responsibilities, but does not clearly define them for all individuals involved in the process including the contractor and TSD managers. It also does not discuss the process to update documentation/configuration or prioritize issues. The document lacks overall detail in the process for steps for filling out change requests and prioritizing those requests, change request documentation requirements, classification definitions, change request communication process, post implementation review, or documentation/configuration updates. The document does not outline all necessary steps for variations in the process to migrate code to production. For

example, manual changes to production (not done through the change control system) were identified during our review, and the document does not define necessary steps to ensure proper controls are implemented.

Without detailed procedures, it is difficult to know what should be happening or identify where improvements or changes need to occur. Procedure documentation also outlines steps to ensure controls are maintained and policies are followed. Therefore, we could not provide assurance policies are followed or consistent between each user involved in each change.

RECOMMENDATION #10

We recommend the Department of Labor and Industry develop a formal change control document that clearly defines all necessary components of its change control process.

Change Control Monitoring Improvements

Industry standards include controls to ensure that the change control process is effective and saving time and cost to the department. The following questions were reviewed to understand how the system is monitored for effectiveness:

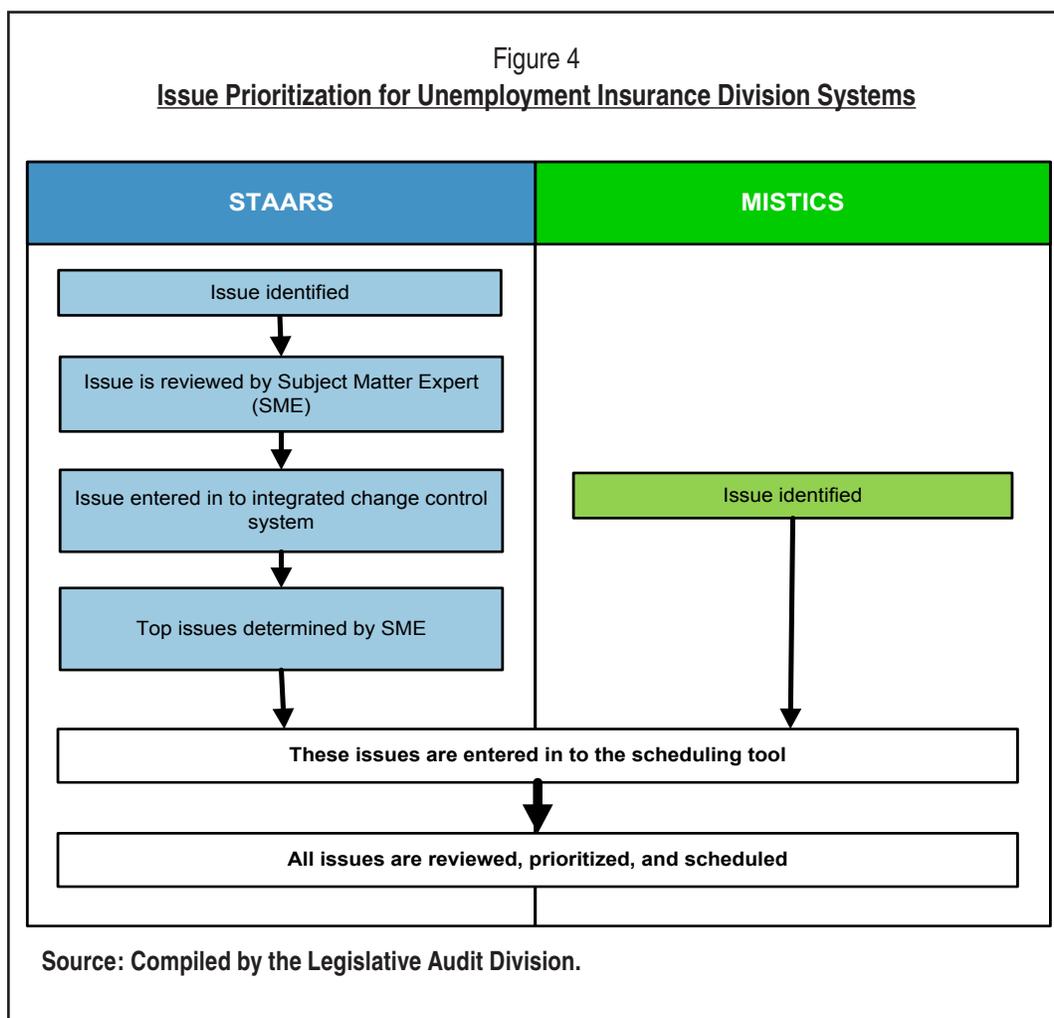
- ◆ Are expectations established for support by the contractor or TSD throughout the maintenance phase of the system?
- ◆ Are metrics to determine effectiveness identified?
- ◆ Are metrics monitored, reported, and reviewed to influence changes to the process?

Industry standards discuss the importance of establishing service level agreements, or service expectations, that consider aspects such as service times, availability, performance, capacity, security, continuity, compliance and regulatory issues, usability, and demand constraints. These are done to increase and maintain user satisfaction with IT services and, more specifically, ensure that change control is effective and supporting users' needs.

During the warranty phase of the project, January 2014 to May 2015, a support plan similar to a service level agreement was in effect. However, after the system was signed over to the state in May 2015, this document, along with the processes for change request reporting and monitoring, is no longer valid.

Since TSD is responsible for managing both STAARS and the system that manages unemployment insurance claims (MISTICS), a User Advisory Board (UAB) was formed and consists of business users from both the claims and contribution divisions within the department. The UAB meets every other week to discuss upcoming priorities and review current work to ensure a balance occurs between the two systems. At these meetings, scheduling for what changes will be implemented for these systems is managed in a project management tool, while the documentation and process for STAARS specific changes are managed within the change control system.

Because both the project management tool and change control system are necessary, a list of high priority change requests are entered into the project management tool as placeholders used for scheduling at the request of the subject matter experts for STAARS. This process is shown in Figure 4.



While the UAB prioritizes changes and modification to STAARS, the department currently does not monitor the service and/or timeliness of changes. During the audit,

the average age of change requests for STAARS was 182 days. Review of the UAB responsibilities and tasks shows that monitoring of change control outside of the current issues being worked on is not completed. Because there are no expectations or monitoring process, it is unknown whether there is an impact to the system users or whether this average number of days is acceptable.

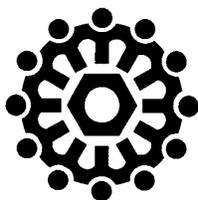
Currently the UAB process is managing the change control process for both systems to managements' satisfaction; however, with TSD staff working on more than one system and multiple projects for the division, there is a business need to set expectations and monitor the efficiency of the change control process. These expectations will not only ensure that issues from each system are addressed timely, but will also assist in further change control process improvements to maximize resources and reduce turnaround.

RECOMMENDATION #11

We recommend the Department of Labor and Industry establish and monitor expectations for changes and modifications to STAARS.

DEPARTMENT OF
LABOR AND INDUSTRY

DEPARTMENT RESPONSE



Montana Department of LABOR & INDUSTRY

Governor Steve Bullock
Commissioner Pam Bucy

Commissioner's Office

September 21, 2016

Mr. Angus Maciver
Legislative Auditor
Legislative Audit Division
P.O. Box 201705
Helena, MT 59620-1705

RECEIVED

SEP 22 2016

LEGISLATIVE AUDIT DIV.

Subject: Information Systems Audit #16DP-01 – Data Integrity of the Status, Tax Accounting, and Rating System (STAARS)

Dear Mr. Maciver:

The Department of Labor and Industry had reviewed the September, 2016 final audit report on the Data Integrity of the Status, Tax Accounting, and Rating System (STAARS), the IT application that supports operations of the Contributions Bureau of the Unemployment Insurance Division. The Department would like to thank your audit staff for their review. The Department has long recognized continuous improvement as a core value in fulfilling our official duties and serving the residents of Montana. We appreciate your office's efforts to help assure we are providing quality services with the best accountability, security and information possible. Our response to your recommendations appear below:

Recommendation #1:

We recommend the Department of Labor and Industry:

- A. Establish and document procedures for granting, reviewing, changing and terminating access, and
- B. Define roles and responsibilities of staff involved in access management and document them within procedures.

Response: The Department concurs with the recommendation. The Department agrees our process for granting, reviewing, changing, and terminating access to STAARS could be strengthened with more formal definition and documentation. Actions already taken to address concerns:

- The role of the systems access administrator for STAARS (and other UI systems) has been transferred to a new position within the division to better align the duties and ensure proper focus and attention is given to systems access management.
- New automated termination process was deployed to STAARS on September 26, 2016. This feature will automatically disable access for users who have been inactive for more than 90 days. Previously, access to STAARS ended whenever a user was removed from the state Active Directory, to which STAARS is connected.

The Department will formalize our access policy and procedure for STAARS and ensure it is well documented with the role of all key players clearly defined by January 2017.

Recommendation #2:

We recommend the Department of Labor and Industry:

- A. Clearly define and document activities the user is allowed to carry out based on the function and which function or role each position should have.
- B. Review the functions assigned to each group on a periodic basis to ensure appropriateness as business process and system changes occur.

Response: The Department concurs with this recommendation. The Department agrees additional documentation and routine review of assigned system functions will reduce the risk of unauthorized actions being performed in the system. Actions already taken to address concerns:

- All instances of over-assigned privileges identified in the system audit have been reviewed and addressed accordingly with the exception of access granted to the Research and Analysis group. The access for R&A is under review and will be addressed appropriately before the end of the year.
- A STAARS system change request is in progress to update and more adequately describe each function number contained in STAARS.

The Department will clearly define and document the functions and roles contained within STAARS by April 2017. A formalized process for periodic review of assigned functions to ensure appropriate user access will be developed and implemented.

Recommendation #3

We recommend the Department of Labor and Industry:

- A. Create documentation of and enforce segregated processes within the system, and
- B. Implement a process to monitor privileged functions including areas where segregation cannot be maintained and users have access beyond their business need.

Response: The Department concurs with this recommendation. The Department agrees enforcing the segregation of duties within STAARS, where applicable, would reduce the risk of potential inappropriate actions being performed in the STAARS system. However, we do maintain there are occasions when granting privileged access is warranted. Actions already taken to address concerns:

- All instances of concern identified in the STAARS system audit have been reviewed and addressed to the extent it did not hinder necessary business activity.

By June 2017, the Department will review business and system processes to ensure appropriate segregation of duties in higher risk areas. Processes will be developed and implemented to monitor instances where privileged access is necessary. Some processes may require system change requests to

accommodate segregation of duties and/or the monitoring of privileged access. Documentation will be drafted clearly outlining the actions the Department determines are privileged and how those will be segregated and/or monitored.

Recommendation #4

We recommend the Department of Labor and Industry increase systematic and manual controls related to NAICS code, custom interest rates, payment agreement abatements, and tax rate changes.

Response: The Department partially concurs with this recommendation. The Department agrees user changes to the NAICS code and tax rate could pose a significant risk to the Department if handled inappropriately, and agree systematic and manual controls should be increased in those areas.

The Department does not, however, believe custom interest rates and/or payment agreement abatements expose the Department to the level of risk required to warrant additional levels of control. MCA 39-51-1301 does not require the Department to assess interest and penalty charges. In the event charge are assessed, MCA 39-51-1303 allows for the abatement (waiver) of all or a portion of the penalty and/or interest charge. Systematic controls already prohibit users from attempting to waive any portion of tax amounts charged. Systematic and manual controls are currently in place to facilitate the review of a significant portion of penalty and interest waivers granted and payment agreement abatements.

With regard to increased controls on NAICS Code changes, actions already taken include:

- A system change request is in progress to mirror the NAICS code input validations contained within the rate document to those validations included in the registration process.
- A system change request is in progress to create a system notification (work item) when a NAICS code is changed after registration. This work item will allow for a review process to occur and adjustments to the rate document to be made if/when necessary.

By June 2017, the Department will review the current business and system practices surrounding the assignment of NAICS codes and submit additional system change requests, where necessary, or implement additional manual controls of the process. In addition, the Department will identify and implement additional controls over manual changes to employer tax rates. These changes may include, but are not limited to, increasing the data contained in the rating adjustment report and formalizing a process for periodic review. Additional system change requests may be required to enhance tax rate change controls.

Recommendation #5

We recommend that the Department of Labor and Industry:

- A. Increase validation and processes concerning invalid and incorrect SSNs, blank last names, and NAICS codes used in rating, and
- B. Document these validations and the procedures uses to remediate any identified errors.

Response: The Department concurs with this recommendation. The Department agrees the integrity of our data is vitally important and there may be opportunities we can explore to further improve the quality. Actions already taken to address concerns:

- The Department reviewed the Social Security Administration requirements for valid SSN characteristics and implemented additional input edits in STAARS to disallow any known invalid SSN. Changes were effective August 12, 2016.
- A system change request is currently being defined to create an ad hoc report of wage records missing last names. A process will be defined and implemented for reviewing and updating these wage records.
- The system change requests identified under recommendation #4 will assist with protecting NAICS code data integrity.

By December 2016, the Department will clearly document all new and existing validation processes and procedures. In addition, by June 2017, the Department will explore additional opportunities for scans or filters within the STAARS system to improve the integrity of our wage record information. The Department has concerns that some of the suggested validations may be resource prohibitive, but we are committed to exploring the possibilities.

Recommendation #6

We recommend the Department of Labor and Industry upgrade the encryption software on field representatives' laptops.

Response: The Department concurs with this recommendation. While the field laptops have always been encrypted, the Department agrees an upgrade to the encryption software was needed. Actions taken to address this concern:

- The encryption software on all field laptops was upgraded to the SITSD supported solution in September, 2016.

Recommendation #7

We recommend the Department of Labor and Industry obtain or develop complete, detailed system documentation that defines:

- A. Processes managed by the system and how users should interact with the system during these processes, and
- B. How the system is expected to function throughout these processes, including any validations or configurations.

Response: The Department partially concurs with this recommendation. The Department agrees system documentation is important and is committed to developing a more detailed user manual for STAARS by expanding and customizing the material provided in the STAARS Help Manager. Since

STAARS is a COTS product and the base product is proprietary in nature, the Department does not agree that it should be responsible for developing detailed system documentation of COTS product system functions, validations or configurations.

Recommendation #8

We recommend the Department of Labor and Industry comply with access management policy by documenting and implementing procedures to grant, review, and terminate access to the change control system.

Response: The Department concurs with the recommendation. The Department agrees our process for granting, reviewing, and terminating access to the STAARS change control system (FCR) could be strengthened with more formal definition and documentation. Actions already taken to address concerns:

- Effective September 2016, a systematic process for auto-terminating inactive users, has been applied to the change control system.

By December 2016, the Department will begin to formalize and document our policy and procedure for granting and maintaining access to the change control system.

Recommendation #9

We recommend the Department of Labor and Industry develop controls to ensure:

- A. The person creating the migration is not allowed to also approve the migration, and
- B. Department staff review changes being made by contractors.

Response: The Department concurs with the recommendation. Actions already taken to address concerns:

- Effective September 7, 2016, an internal policy was communicated to all contracted personnel as well as internal developers regarding the approval of migrations to STAARS production. Going forward, migration approvals will be done by a state developer and the approver will not be the same individual who submitted the migration.

Recommendation #10

We recommend the Department of Labor and Industry develop a formal change control document that clearly defines all necessary components of its change control process.

Response: The Department concurs with the recommendation. The Department agrees our change control process for STAARS could be strengthened with more detailed documentation.

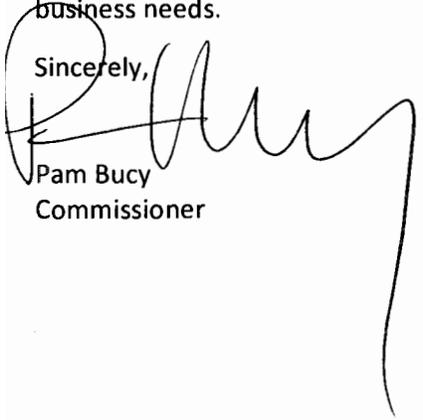
The Department will review its current STAARS change control policy and procedure and add additional details regarding the specific process and the roles and responsibilities of those involved by April 2017.

Recommendation #11

Establish and monitor expectations for changes and modifications to STAARS.

Response: The Department concurs with the recommendation. LAD correctly notes the department's satisfaction with the current process. Nonetheless, there is always room for improvement. The department will review the effectiveness of the UAB, the STAARS change control system (FCR), and Contributions staff routine review and prioritization of change requires to meet near-term and strategic business needs.

Sincerely,

A handwritten signature in black ink, appearing to read 'Pam Bucy', written over the typed name.

Pam Bucy
Commissioner