INTERNAL AUDIT REPORT

Payroll Management

R-19-07

June 1, 2020

This record contains information that is classified as protected pursuant to Utah Code 63G-2-305(12). This record may not be released without appropriate authorization from a UTA records officer.
This information has been redacted from this report.

Executive Summary

Introduction

In conjunction with the UTA Audit Committee, Internal Audit (IA) developed a risk-based annual audit plan. All of the audits on the audit plan are conducted in accordance with the International Standards for the Professional Practice of Internal Audit, published by the Institute for Internal Auditors (IIA), and provide several benefits:

- Management's continuous improvement efforts are enhanced
- Compliance is verified and shortfalls are identified so that they can be corrected
- Oversight of governance, control and risk management is strengthened

As part of the 2019 internal audit plan, IA was directed by the Audit Committee to perform an audit to determine if controls over payroll management are designed adequately and operating effectively to ensure compliance with key federal regulations, state laws, and internal policies and procedures as well as to support the achievement of management objectives. The preliminary stage of the audit was concluded in March 2018 and the final audit was completed in December 2019.

Background and Functional Overview

Management provided a functional overview of the timekeeping and payroll processes to provide context to this report. Please note that all of the statements made are assertions by Management and were not assessed by Internal Audit.

UTA's payroll function pays between 2,500-3,000 employees bi-weekly, 26 times a year. The Authorities' employees are made up of administration employees and bargaining unit employees. Bargaining unit employee pay policies are covered by the Collective Bargaining Agreement, while administration employee pay policies are covered by the personnel policy. Employees are responsible for having their time entered and approved by the Monday morning of a payroll week. The payroll process is responsible for making sure all employees are paid correctly (according to the approved time entered) and on time each pay period. This process is dependent on many hard working groups imputing and reconciling 4 different timecard modules throughout the company into one payroll system.

The Payroll group, which is part of the Accounting department, is responsible for payroll processing and works diligently with many other groups to coordinate that payroll gets out each pay period. The various groups include HR, who set up the employee's information, supervisors and managers who review and approve time in various systems and office specialists who remit timesheets and information to Payroll. The timekeeping systems outside of the Enterprise Resource Planning system (ERP) are maintained by various groups in Operations Analysis and Support and Customer Service who make sure the systems that are used for time entry are properly functioning and reporting. The 4 systems used to gather and calculate employee time entered and pay rates are as follows:

- TC-1 – 340 maintenance and customer service employees
- OWATS – 1,125 operations staff
- Paper time cards – 220 train hosts, trainers, LR MTC staff, and system monitor employees
- ERP – 850 administrative employees

TC-1, OWATS, and the paper time cards are loaded into the ERP for final processing and payment generation.

Some initiatives, which have been put in place to improve timeliness and accuracy, include:

- Deadlines for employee information set up and changes

- Deadlines for time entry and approval
- Deadlines for division time remittance
- Check figure to ensure number of employees and hours remitted are loaded correctly
- Numerous variance reports are generated and reviewed for a number of criteria, prior to payments going out. This is to catch any mistake or anomalies that may come through in processing
- Employees are given paystubs to review for accuracy and payroll correction memos are available to remit any identified corrections

The performance goal of the payroll process is to pay every eligible employee correctly and on time, all 26 pay periods each year. UTA's current payroll staffing level can only allow for minimal rework of timecards in the cases where employees are paid incorrectly for the pay period, so the tolerance for errors or omissions are not possible.

Yearly our external auditors review payroll when they perform their annual audit and test controls as they relate to current policies. Utah State Work Force Services has also reviewed the payroll policies, and worker compensation classes and rates in the past. No findings have been noted by any of these groups.

Objectives and Scope

The period of the preliminary assessment was January 1, 2017, through December 31, 2017 with the completion of the audit work focusing on January 1, 2019 through July 31, 2019.

The primary areas of focus for the payroll audit were:

- Governance
- Payroll accounting and payments
- People Office, Total Rewards, and HR Services & Labor Relations, as it relates to the payroll process
- Payroll processing
- Enterprise resource planning system (ERP) master files, as it relates to the payroll process
- Bargaining Unit employee timekeeping
- Bargaining Unit timekeeping application administration

Internal audit excluded from the scope of this audit areas such as:

- Compliance with the Collective Bargaining Agreement, with the exception of potential impact on certain timekeeping and payroll controls
- Withholding calculations (taxes)
- W-2 reporting
- Compliance with the Fair Labor Standards Act (FLSA)

Audit Conclusion

Conclusion

The audit revealed that Management made progress in addressing risks identified in the preliminary assessment by adding more structure such as implementing stronger payroll and timekeeping policies and standard operating procedures for UTA overall. Standard operating procedures were also created for the various timekeeping applications used outside of the Enterprise Resource Planning system.

As a result of the work Management performed since the preliminary assessment was completed, Internal Audit was in a position to assess the remaining risk in more detail and add additional recommendations to mitigate those risks.

In summary, the audit found that [redacted] had abilities within the Enterprise Resource Planning system unrelated to payroll processing, which included employee masterfile creation and changes as well as payment and banking activities. The risks related to these abilities were elevated considering that oversight and monitoring controls for changes to master data, and the processing and payment of interim checks were not established.

The overall responsibility for timekeeping systems was not assigned, which resulted in a risk that the systems were not adequately administered or maintained. A legacy timekeeping system that was planned to be replaced prior to the assessment had still not been replaced at the time of the audit nor was a clear timeline for its replacement available.

Further work needed to be done on the operations timekeeping systems, including incorporating in the standard operating procedures an independent review and approval procedure for operator timekeeping, and assessing the practices that the legacy timekeeping system used for facilities maintenance, customer service, and other personnel.

While this report details the results of the audit based on limited sample testing, the responsibility for the maintenance of an effective system of internal control and the prevention and detection of irregularities and fraud rests with management.

Internal Audit would like to thank management and staff for their co-operation and assistance during the audit.

Table of Contents

APPENDIX 1

Index of Findings

APPENDIX 1

1. Payroll Process Governance

Preliminary Finding R-18-1-1	High

Criteria:

Enterprise governance is an overarching system, which seeks to align priorities, funding, and resources and elevates decision-making responsibility, authority, and accountability to the appropriate levels. Governance principles include:

- Management establishes reporting lines, with board oversight, of the development and performance of internal control
- Individual accountability is in place for internal control responsibilities that support entity objectives

Sources:
COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes, Robert R Moeller
COSO: How the COSO Frameworks Can Help, James DeLoach and Jeff Thomson

Condition:

UTA payroll processing required coordination and input from multiple business units, departments and divisions. The assessment found that there was no corporate level policy laying out the roles and responsibilities of each participant in the process. Some examples of areas which lacked the establishment of roles, responsibilities and accountability, included:

- Responsibility for data and applications between People Office, Payroll, business units and the Operations and Analysis division was not defined, [redacted]
- Responsibility for 457 plan procedures were not defined, including the accuracy and validity of the calculation and subsequent payments between Payroll, Accounting and People Office
- Responsibility for timecard and leave accuracy, approval, and retention between business units, divisions, and Payroll administration was not defined
  - The majority of UTA timecards [redacted] to ensure accuracy and validity prior to payroll processing
  - Payroll administrators entered over 200 Bargaining Unit manual timecards each pay period, in addition to carrying out their payroll processing responsibilities
  - While Payroll retained copies of printed and manual timecards, and some business units retained copies as well, overall responsibility for timecard retention was not assigned in a policy
  - Copies of four timecards requested in conjunction with the assessment were not provided

Root/Cause Analysis:

- Payroll processes, roles and responsibilities developed over time, as business needs arose
- Management relied on the expertise of existing staff rather than oversight in the form of written governance

Effect:

- Payroll administrator time may not be used most efficiently
- UTA and employees are unprotected in the event of errors, omissions, and accusations of wrong doing

APPENDIX 1

Recommendations

- People Office, Accounting, Payroll, division, department and business units payroll responsibility, authority, and accountability should be established in a Corporate level policy, including the following:
  - Employee timecards and leave accuracy, approval and retention
  - ERP and timekeeping data and applications, including user access rights
- The policy should be reviewed and updated on at least an annual basis to ensure it remains relevant

Management Agreement	Owner	Target Completion Date
Yes	Chief Financial Officer	September 30, 2018

Accounting accepts responsibility for establishing a corporate-wide policy that will serve as a coordination document with the Chief People Office, IT, and designated Operations personnel in charge of timekeeping. Accounting has already begun meeting and brainstorming processes that would provide for segregation of duties and guaranteed accuracy of the payroll process.

Final Status	**High**

Implemented:

- The responsibility, authority, and accountability of the payroll process was found to be better established through the design and implementation of policy 3.1.10 Pay Processing and Management and 3.1.10 Pay Processing and Management Procedures.
- The following responsibilities were found to be specifically assigned
  - ERP data and user access rights
  - Responsibility to calculate 457 benefits
  - Employee timecards and leave accuracy, approval, and retention

The following items represent areas of continued risk:

- Outside of user access there was a lack of defined roles and responsibilities identified in policies and procedures for ownership of the Maintenance and Operator timekeeping systems between Analysis and Solutions (OAS); Operations; Accounting, and others
- [redacted]
- No procedures [redacted] outside of changes to the CBA identified by Labor Relations, had been created by Benefits and Compliance office

Segregation of duties risks

Segregation of duties is one of the fundamental building blocks of internal controls and its inclusion in control design mitigates errors as well as fraud risk. Functions within a process to be separated for adequate segregation of duties include initiation, custody, recording, and reconciling. For example, in an ideal environment an employee would enter their time, their supervisor would review the employee's time entry to confirm it reflects what was worked, Payroll would process the approved instructions without any adjustments, and Accounting would reconcile the accounts.

Where segregation of duties is not practical, management selects and develops alternative control activities. (COSO Integrated Framework, 2013).

APPENDIX 1

A number of responsibilities assigned to Payroll personnel by policy would generally be seen as HR responsibilities due to underlying accountability of the processes falling under People Office, including:

- Significant segregation of duties concerns included the payroll staff each having had the ability to process payroll as well as add new employees, create payments, create positive pay files, and enter direct deposit information
- processing non-Department of Transportation (DOT) verifications of employment
- calculation of:
  - 457 match at year end and at termination
  - severance payments
  - pay adjustments from HR memos on pay rates and benefit pay adjustments
- Checks to benefits providers are currently processed by the Payroll Department but should follow the AP process as they are payments to vendors

Recommendations

- A risk assessment should be performed to identify key risks in the payroll process and design mitigating controls, with specific emphasis on roles and responsibilities. The risk assessment should incorporate the functioning of the ERP, where relevant to the payroll process
- Management should limit payroll personnel system abilities, based on the results of the risk assessment, to those needed to perform their responsibilities. Where additional access is needed and presents risk, management should consider compensating controls such as periodic monitoring of activities and read only access
- Ownership of each timekeeping application should be fully assigned to a logical owner who is responsible for the employee timekeeping performed on that application. Identified owners should assign administrative responsibility for each system as well as define roles for administrators. The results of the risk assessment should aid in addressing this recommendation
- Roles and responsibilities for all pay code changes should be assigned and procedures implemented that include review and approval of changes to ensure that they are valid, complete, and correct
- Responsibility for performing all employment verifications (both DOT and Non-DOT) as well as assuring correct calculation of 457 matches, severance payments, and pay adjustments related to HR issues should be assigned clearly by HR
- Checks to benefit providers should be routed through Accounts Payable, identical to all other vendor payments

Management Agreement	Owner	Target Completion Date
Yes	Chief Financial Officer	December 31, 2020

- The payroll group and the CPO's ERP specialist will perform a risk assessment with a specific emphasis on roles and responsibilities and use the results to better align access and internal controls
- Timekeeping ownership is being clarified as we put Kronos into production scheduled for July 2020. Payroll has been working closely with the CPO staff to provide more documentation and gain approval on pay and benefit code changes and additions
- Non-DOT employment verifications are still being performed by the payroll department with any non-pay questions being sent to the people's office

- Payroll is in the beginning phases of exploring what would be required to have AP take over benefit provider payments

2. Accounting and Payments

Preliminary Finding R-18-1-2	High

Criteria:

- Accounting Manual 6 “Payroll Accounting and Controls” Section 6.5 states, “Payroll transactions have a separate bank account and require reconciliation on a monthly basis. This reconciliation is prepared by the staff accountant and includes a list of outstanding transactions due to timing. Checks were void if not cashed within 90 days of the date of issuance. The staff accountant is responsible for notifying employees and/or vendors when transactions were not cleared within the 90 days. If the accountant is not able to clear the transaction within 180 days, the funds will be transmitted to the State of Utah as unclaimed property.”
- Accounting SOP ACC-006, Section 6.6, states, “The payroll liability accounts were reconciled once a quarter by one of the Accountants. As a general internal control, account reconciliation assignments were rotated on an annual basis. The Assistant Comptroller reviews the reconciliations on a quarterly basis.”
- Accounting Manual 6 “Payroll Accounting and Controls” stated, “The ACH request form must be authorized by a signer on the account in order for the ACH to be funded. The only authorized signers are the President/CEO; Vice President, Finance; Comptroller; and Deputy Treasurer. Normally the Comptroller reviews and signs off on the payroll ACH request. In absence of the Comptroller, the Deputy Treasurer performs this review. Once approved, the ACH request form is sent to the bank and the funds are released to employees’ bank accounts.”
- The Accounting Procedure Payroll manual stated that a “comprehensive annual review of the manual will be conducted in the third quarter of each fiscal year to ensure it reflects current policies and procedures.”

Condition:

IA reviewed payroll-related accounting functions, including the payroll bank account reconciliation process and oversight of ACH payments and journal entries. The review found the following:

- Employees and benefit providers were paid using ACH payments. IA confirmed that the Comptroller reviewed and signed off on the ACH report. However, the Comptroller’s review was based on perceived reasonability of the payment amount and did not include a more meaningful review, such as reviewing a sample of payments or unusual payment amounts and corresponding documentation. IA also noted that Payroll was notified when ACH transactions are rejected, but there was no follow-up performed to ensure that ACH errors are resolved
- IA reviewed the payroll bank account reconciliations for May, November, and December 2017 and noted the following:
  - The Comptroller had not initialed one of three reconciliations after review and one review was not dated
  - Reconciliations included the checks that had been outstanding longer than 180 days, including six stale checks on the May 2017 reconciliation and four on the December 2017 reconciliation

APPENDIX 1

  - The May 2017 reconciliation general ledger balance did not agree with the ERP system balance seeing that it did not include subsequent journal entries
  - While the detail activity and ending balance on the December reconciliation was correct, the debit and credit summary totals had been brought forward from the November 2017 bank statement in error
- The payroll process kicked off a series of automated journal entries. Manual journal entries were performed but did not go through a documented review and approval process prior to posting for two of the three months sampled and evidence supporting journal entries was not retained
- 457 UTA match calculations were verbally conveyed to the Senior Accountant by Total Rewards, rather than through written documentation, resulting in a weak audit trail. In addition, a system report produced from the ERP system for 457 UTA matching amounts was unreliable for some employees and contributions were not reconciled
- Reconciliations of payroll-related balance sheet accounts, with the exception of the payroll bank account, occurred annually, not quarterly as indicated in Accounting's standard operating procedure
- No payroll liability reconciliations were performed in 2017. However, a reconciliation of 2017 activity was expected to be completed by February 2018
- Timing and responsibility for VERTEX updates to the ERP system tax withholding table was not clear and no monitoring was in place to ensure that changes were up-to-date
- The Accounting Procedure Payroll manual stated that a "review of the manual will be conducted in the third quarter of each fiscal year to ensure it reflects current policies and procedures." However, Accounting policies were more than one year old and have not been reviewed in line with the manual

Root/Cause Analysis:

- Accounting and payroll processes, roles and responsibilities have developed over time, as business needs arose, in conjunction with turnover in comptroller staffing during the audit period
- Management relied on the expertise of existing staff rather than oversight in the form of written governance

Effect:

Errors and omissions were more likely to occur. For example, a net overpayment of $25.5K 457 matching bonus was made. The error was detected by a UTA employee and not through internal controls. UTA is at increased risk of this and similar errors in the absence of additional controls.

Recommendations

Accounting's standard operating procedures should be reviewed and updated to include procedures, required documentation, review and approval of the following key payroll processes:

- ACH payment accuracy, validity and completeness
- Bank account reconciliations
- Stale dated checks
- Automatic and manual journal entries
- 457 UTA match calculations and accounting
- Reconciliations of payroll-related balance sheet accounts
- Timing and responsibility for the ERP System tax withholding table updates

APPENDIX 1

Management Agreement	Owner	Target Completion Date
Yes	Chief Financial Officer	August 31, 2018

Accounting's payroll staff will review standard operating procedures and update the procedures to reflect current operations and understandings. Accounting over the next few months will redistribute reconciliation and banking work amongst existing staff and provide for more diligent oversight, approval, and system testing for payroll.

Final Status	**High**

Improvements were noted in the following areas for procedures, required documentation, review and approval:

- System control implemented to require independent approval of journal entries
- ERP System tax withholding table updates
- Bank account reconciliations
- Stale dated checks

IA noted the following areas of risk outstanding:

- ACH
  - ACH payment review and audit trail requirements had not been documented in governance documentation such as policies or standard operating procedures
  - A formal process could not be identified, such as a comprehensive independent review, to verify the accuracy, validity, and completeness of ACH payments as follow up on ACH errors was an ad hoc process on a case by case basis
- Bank Account Reconciliations and Stale Checks
  - Outstanding deposits included an item going back to June 2018 and 3 items from January 2019 for both the April 2019 and June 2019 bank reconciliation for account 1.10101
  - Stale dated check documentation support was not defined for evidencing follow up or remittance
- 457 UTA match calculations and accounting did not include any review or approval process, or any requirement for one
- Reconciliations of payroll-related balance sheet accounts
  - The payroll related balance sheet reconciliation performed by the Senior Accountant is not reviewed or approved. This was likely due to the absence of a documented requirement for review and approval, including the requirement for documentation to support payroll liability account reconciliations
  - Testing revealed that for one sampled pay period, reconciliation balances tested were agreed to standard payroll processing activity. However, 7 (of the 22) reconciliations tested could not be agreed to the overall general ledger balance, which included items outside the standard payroll process, resulting in non-detection of reconciling items
- Timing and responsibility for the ERP System tax withholding table updates was not found in the payroll governance documentation

Recommendations:

- ACH payment review standards and document retention requirements should be documented in Accounting department policy or procedures

APPENDIX 1

- Outstanding deposits greater than 1 month should be investigated and remediated. Where investigation and remediation need additional time, updates should documented on the account reconciliation to inform reviewers of status and progress of unreconciled deposit
- Payroll should confirm documented HR management review and approval for the 457 match calculation prior to completing the process in the system. This should be incorporated in the policies and procedures
- The existing payroll balance sheet reconciliation process should be modified to include the entire account balance as well as a review and sign off to monitor completeness of the reconciliations and timely follow up on outstanding items
- Timing requirements should be added to departmental policies or procedures for tax table updates to comply with applicable laws and regulations
- The documentation needed to support stale dated check processes should be included in the Accounting Policy Manual

Management Agreement	Owner	Target Completion Date
Yes	Chief Financial Officer	December 31, 2020

- ACH payment review section will be updated in the payroll policies manual
- A process will be created with action steps for reviewing and remediating deposits older than 1 month
- For the 457 match calculation the Senior Accountant will work closely with Total Rewards staff on the calculation and retain written approval from both groups
- More detailed balance sheet reconciliations will be created with timely follow up on outstanding items
- A section will be added to the payroll policies manual for timing and type of tax table updates
- The stale dated check documentation will be added to the payroll manual

3. People Office

Preliminary Finding R-18-1-3	**High**

Criteria:

- Enterprise governance is an overarching system, which seeks to align priorities, funding, and resources and elevates decision-making responsibility, authority, and accountability to the appropriate levels. Governance principles include:
  - Management establishes reporting lines, with board oversight, of the development and performance of internal control
  - Individual accountability is in place for internal control responsibilities that support entity objectives
- COSO Framework stipulates control activities should be deployed through policies that establish what is expected and procedures that put policies into action

Sources:
COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes, Robert R Moeller
COSO: How the COSO Frameworks Can Help, James DeLoach and Jeff Thomson

- Utah Transit Authority Technology Office, No. 11.1.0, ERP Technology Standard Operating Procedure (SOP) states in section IV User access rights states, *"D. End User Access Review*

APPENDIX 1

Procedure 1. On a Quarterly basis… the ERP Developer will email the designated Super Users the following to be reviewed ... A list of all roles used in their area of responsibility, with sensitive roles being highlighted… [and]... A list of all Users in each role…Unless otherwise specified, the Super User will have one week to respond with either changes or acknowledgement that the report was correct.”

Condition:

- There were no standard operating procedures regarding the application of the Collective Bargaining Agreement
- [redacted]
- Responsibility for interpreting and overseeing the consistent application of Collective Bargaining Unit Agreement (CBA) compensation rules were not defined
- Responsibility for benefit accrual codes, benefit deductions, benefit reconciliations, and payments to benefit providers between Payroll, Accounting and Total Rewards were not defined
- The same Total Rewards employee that entered deductions for health insurance and other benefits also reconciled amounts billed by providers, resulting in poor segregation of duties
- There was no review in place to ensure that employee deductions were valid or accurate
- Responsibility for aspects of 457 accrual and matching payments were not well defined and, as noted previously, Total Rewards verbally conveyed UTA’s matching contribution to Accounting
- Oversight of master data changes was not adequate. The ERP Technology Systems Admin in Total Rewards maintained tables of pay codes (types of time such as overtime and straight time, as well as accruals, benefits, deductions, and automatic accounting instructions). Changes were manually tracked on an Excel spreadsheet, along with screen shots from the system. However, there was no formal request process for making changes to the master data and no monitoring oversight, review [redacted]
- [redacted]

Root/Cause Analysis:

- The People Office processes, roles and responsibilities were developed over time, as business needs arose
- While the People Office had developed multiple standard operating procedures, some key areas were not included or had changed over time
- [redacted]

Effect:

- [redacted]
- [redacted]

APPENDIX 1

- [redacted]
- [redacted]

Recommendations

- People Office and Payroll roles and responsibilities should be reviewed and aligned to strengthen segregation of duties
- People Office standard operating procedures should be reviewed and updated to include:
    - A process for the consistent interpretation and application of the Collective Bargaining Agreement compensation rules
    - [redacted]
    - Maintenance, accuracy, and validity of benefit accruals and accrual codes
    - Benefit deductions, benefit reconciliations, and payments to benefit providers
    - Roles and responsibilities for entering deductions for health insurance and other benefits, reconciliations of amounts deducted to amounts billed, and review that employee deductions are valid or accurate
    - Roles and responsibilities for 457 accrual and matching payments
    - [redacted]
    - [redacted]

Management Agreement	Owner	Target Completion Date
Yes	Chief People Officer	August 1, 2018

Labor Relations in consultation with the ERP Systems Administrator will develop a standard operating procedure that will document in writing how the Systems Administrator will be informed of changes to the CBA. Changes will be communicated in a written document with clear examples of how to apply the change. This will be complete by August 1, 2018 by the Director of HR Services and Labor Relations, HR Business Partner and the ERP Technology Systems Admin.

ERP Systems Administrator and the Benefits and Compliance Manger in consultation with internal customers will develop an SOP that outlines how system changes need to be authorized, requested monitored & audited. This will be completed by August 1, 2018 by the Director of Total Rewards, the Benefits and Compliance Manager and the ERP Technology Systems Admin.

People Office currently has HR 810, HR820 and HR 830 in place that outline the process for enrolling and terminating an employee benefit, reconciling the monthly bills to the benefits vendors as well as making deposit and disbursements into and from the Joint Insurance Account which the bargaining unit bills are paid. The Benefits Administrator, the Benefits and Compliance Manager, and the Chief People Officer will review these SOP for accuracy and update if needed by July 1, 2018.

A standard operating procedure is in development to address how one-time-overrides are done which defines roles and responsibilities. The Benefits Administrator will update this by July 1, 2018.

APPENDIX 1

Roles and responsibilities for 457 accrual and matching payments. The Benefits Administrators in consultation with accounting and the Benefits and Compliance Manger will determine the new process and develop Standard Operating Procedures to outline the process. The Benefits Administrator, the Benefits and Compliance Manager and the Comptroller will complete this by August 1, 2018.

Cleanup of the Security Report has been completed and a quarterly audit will be performed at the end of each quarter. Quarter one audit for 2018 has been completed.

Final Status	**High**

Implemented:

- Management implemented a review process for user access to HRIS applications and data
- Collective Bargaining Agreement (CBA) changes to HRIS was assigned through the implementation of policy 3.1.10 Payroll Processing Management and 3.1.10 Pay Processing and Management Procedures
- Supervisor training includes self-identification by Labor Relations as responsible for CBA interpretation

Partially Implemented:

- Total Rewards and Payroll roles and responsibilities were reviewed by the Comptroller and aligned to strengthen segregation of duties, however some SOD risks were identified below as well as in finding 1

Audit procedures revealed the following risks:

- [redacted]
- Roles and responsibilities related to benefit deductions (e.g. health insurance), related reconciliations, and review of employee deductions were not assigned
- Roles and responsibilities for 457 accrual and matching payments have not been defined

Audit test results revealed the following:

- [redacted]
- [redacted]

Recommendations

- [redacted]
- [redacted]

APPENDIX 1

- [redacted]
- An owner should be assigned to oversee that a benefit reconciliation process is designed, implemented, and monitored to assure that benefits and deduction amounts are correctly calculated or applied, which should include a management review
- An owner should be assigned to calculate 457 accrual and matching payments and a process should be designed to assure that calculations are timely, complete, and correct prior to submission to the payroll department.
- [redacted]
- Management should review existing HR SOPs implemented to confirm that the current process and the SOPs are aligned

,Management Agreement	Owner	Target Completion Date
Yes	Chief People Officer	July 31, 2020

Management will take the following actions:

- Approval Process for Pay Codes
  - The process will be changed to ensure there is an electronic record of all pay code requests and approvals. The HRIS Administrator will facilitate an email request to the Manager of Total Rewards, and approval/denial will be provided for applicable pay codes. The HRIS Administrator will document the requestor and approver on a Spread Sheet to ensure an overall record is kept for these requests.
- Benefit Payment/Reconciliation Duties
  - The Sr. Benefits Administrator will prepare and reconcile the monthly benefits payments for both bargaining and admin. Once prepared, these will be forwarded to the Manager of Total Rewards for a final review and reconciliation before they will be signed. Once approved the Sr. Benefits Administrator will retain a record of approval.
- 457 Match Review/Approval
  - The Finance Department will calculate and prepare the annual 457 Matches for those who have participated and qualify for the match. Once the calculations have been completed, a sample will be forwarded to the Total Rewards Team to be spot-checked. The goal is to spot-check a 10% sample to ensure calculations have been completed accurately.
- SOP Review
  - HR SOP's will be reviewed and edited to ensure compliance as required. The overall goal is to review all HR SOP's by 12/31/2021 to ensure they reflect correct duties, parties responsible, and governance.
- [redacted]
  - [redacted]

APPENDIX 1

4. Payroll Processing

Preliminary Finding R-18-1-4	High

Criteria:

- Enterprise governance is an overarching system, which seeks to align priorities, funding, and resources and elevates decision-making responsibility, authority, and accountability to the appropriate levels. Governance principles include:
  - Management establishes reporting lines, with board oversight, of the development and performance of internal control
  - Individual accountability is in place for internal control responsibilities that support entity objectives
- COSO Framework stipulates control activities should be deployed through policies that establish what is expected and procedures that put policies into action

Sources:
COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes, Robert R Moeller
COSO: How the COSO Frameworks Can Help, James DeLoach and Jeff Thomson

Condition:

- Segregation of duties, oversight and physical controls over payroll processing were not adequate.
- Not all payroll roles and responsibilities were properly segregated:
  - Payroll administrators had responsibilities that include ad/hoc ERP timecard entry and approval for administrative employees, creating and printing checks, input and review of direct deposit information, making adjustments to employee pay, and entering wage attachments and deductions
  - Payroll administrators had super user access to Payroll and Human Resource ERP data and applications
- Payroll administrators monitored their work each pay period by completing a standardized checklist and signing off on key tasks. They also produced and reviewed a series of exception reports. However, IA noted that not all key items were included on the checklist and one out of three selected for review was not fully completed. IA also noted that some exception reports were retained, while others were not retained. Those retained did not always include evidence that they were reviewed and followed up on. Finally, exception reports for potential errors such as employees paid before their start date, were not in place
- Some controls were performed visually, and therefore, lacked a sufficient audit trail to support their effectiveness, including the following:
  - [redacted]
  - Comparison of gross pay for administrative employees to that of the prior period
  - Comparison of benefit payment amounts to system generated reports
  - Exception reports for employees paid less than $500 and pay related to terminated employees
- There was not always adequate documentation to support payroll adjustments. Business units generally completed a payroll adjustment memo, signed by a supervisor, when requesting an employee pay correction. Other corrections, such as those initiated by Payroll, did not require an adjustment form. IA reviewed a sample of 24 payments made outside the normal payroll process and noted examples of adjustments that were lacking adequate documentation, such as:
  - In one instance, People Office entered a benefit deduction in error that was more than the employee's paycheck. Employee pay was done on an interim check. While Payroll staff was

APPENDIX 1

able to provide an explanation, IA noted a lack of clear documentation, such as system notes or a form used by Payroll and/or People Office, documenting what occurred and what steps were taken to fix the problem

- In another instance, according to the Payroll administrator, an interim check was issued to process time submitted to Payroll late. However, there was no email or other correspondence to support that the submission was late. The Payroll administrator did not retain all related emails once the payroll was processed
- A correction was required after People Office changed an employee's pay rate to the wrong amount and then corrected it later, impacting two paychecks. IA noted a lack of clear documentation, such as system notes or a form used by Payroll and/or People Office, documenting what occurred and what steps were taken to fix the problem
- [redacted]

- Payroll administrators did not retain all emails supporting the submission of timecards and other correspondence regarding payroll. An email regarding the completeness of Bargaining Unit TC-1 employee timecards was not in place for the entire audit period
- Oversight, review and approval of payroll processing and documentation was not adequate, including review and approval of interim checks, adjustments, overrides, wage attachments, direct deposit account changes, exception reports and checklists
- There was no business unit, department, or division review and approval of the accuracy of ERP payroll data or overall roster of employees paid
- There was no control in place to ensure that all garnishments entered into payroll were reviewed by the Office of General Counsel
- There were no standard operating procedures regarding timecard approvals, deadlines for payroll processing or required follow-up and accountability
- [redacted]
- IA also noted that payroll processing included several time-consuming, manual procedures which increased the likelihood of errors or omissions, including:
  - Each pay period, Payroll administrators printed, organized and distributed over 2,000 paychecks and paystubs
  - Light Rail maintenance, train hosts and trainees, Maintenance of Way, TVM maintenance, and system monitors used manual timecards. As mentioned in Finding 1, for every pay cycle Payroll administrators entered over 200 manual timecards
  - Each pay period the Payroll administrator manually separated a UTA-wide leave balance report from ERP into individual reports for each business unit and then manually distributed the individual files by email to office specialists and other payroll contacts
- [redacted]

Root/Cause Analysis:

- Payroll processes, roles, and responsibilities developed over time, as business needs arose
- Collective Bargaining Agreement rules and the nature of work performed may have fostered the development of satellite timekeeping system and manual timecards
- Management relied on the expertise of existing staff rather than oversight in the form of written governance or oversight
- Turn-over in key personnel

APPENDIX 1

Effect:

- Errors and omissions in payroll processing are more likely to occur
- Employees are left unprotected against false accusations
- Pay disputes may arise where documentation is inadequate
- Current manual procedures may not be the best use of payroll resources and Payroll administrator staff time

Recommendations

Management should design and implement Standard Operating Procedures that include:

- Key tasks that should be included on payroll checklists each pay cycle
- Supporting documentation that should be retained for items on the checklist
- Required retention periods for payroll documentation, including electronic communication such as email
- A method for identifying, reviewing and approving actions taken by [redacted]
- Adequate segregation of duties or compensating controls, such as periodic reviews
- Procedures and documentation requirements for adjustments
- Assign and perform reviews of access controls over payroll data and applications

Management should:

- Update or reassign manual processes, such as providing employees with a record of their pay stub and communicating leave balances
- Implement increased physical controls over check printing and payroll processing

Management Agreement	Owner	Target Completion Date
Yes	Chief Financial Officer	December 31, 2018

Accounting's payroll staff will develop a more robust payroll checklist and clear approval and oversight rules for procedures internal to Accounting. [redacted]

Final Status	High

Implemented:
Management expanded the existing payroll process guidance to include more key controls as well as timing and documentation/reporting requirements for completing the process.

Additional work is needed to mitigate the risk related to the following:

- [redacted]
    - [redacted]
    - [redacted]

APPENDIX 1

  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

  The items below, either on their own or in conjunction with others, represented risk due to inadequate segregation of duties:

  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

- Payments
  - [redacted]
  - [redacted]
  - [redacted]
- Checks
  - Paper check distribution did not have any formal standards and controls. Due to new hires and employees without bank accounts, some non-interim checks were still printed and distributed. IA noted 70 (out of 3321) non-interim checks, or 2%, were printed for the pay period ending (PPE) 07/27/19
  - Employees with payroll activity but no net pay did not receive paystubs which increased the risk that activities that result in changes to gross pay, benefits payments, or taxes were not communicated

APPENDIX 1

  - Payroll did not perform a review or analytic to determine if all employees who had payroll activity received a paystub

- Testing of a sample of 25 interim checks revealed:
  - [redacted]

- Interim Payments
  - [redacted]

Recommendations:

- Management should evaluate Payroll personnel responsibilities for adequate segregation of duties and where possible, remove responsibilities and security access that does not relate to the department's responsibilities. Where segregation of duties issues persist management should institute monitoring controls using existing monitoring software to determine whether transactions are correct, complete, and valid
- Where the ERP system is unable to report critical information a monitoring process should be created that incorporates the existing monitoring software to determine things such as whether payments are being initiated [redacted] appropriately
- [redacted]
- Payroll processes should be updated to align with any changes management makes to the process, e.g. should management follow the recommendation to establish requirements for interim check processing then policies and procedures should be updated accordingly
- All employees with payroll activity should receive a paystub with the results, not just employees with net pay. To ensure this, a review of pay stub distributions should be put in place to determine if all employees who had payroll activity received a pay stub

Management Agreement	Owner	Target Completion Date
Yes	Chief Financial Officer	December 31, 2020

- The payroll group and Accounting's ERP specialists will work on restricting access where it is not needed and formulating a way to track changes in areas of high risk. A number of areas that payroll personal had unneeded access has already been removed
- Payroll will look into a way to track payroll checks from creation to delivery, with an employee signature being required upon receipt
- A policy for interim checks is currently drafted. Payroll process will be updated when applicable.
- Payroll will research a way to get all paystubs regardless of net pay amount

APPENDIX 1

5. ERP System Master Files

Preliminary Finding R-18-1-5	Medium

Criteria:
Utah Transit Authority Technology Office, No. 11.1.0, ERP Technology Standard Operating Procedure (SOP) states in section IV, "*C. New User Creation Procedure… The User, manager, supervisor or office coordinator will request that rights be granted via an e-mail to the Help Desk, or by entering their own POB ticket… A complete ERP Security Change Form must accompany the POB request. This form can be found on SharePoint on the Technology Page.*"

Condition:
ERP access forms were not always completed. IA requested ERP access forms for five users hired during 2017 that had ERP access rights to sensitive information. A signed form was not on file for 3 out of 5 employees.

Root/Cause Analysis:

- The Technology Office ERP System Developer stated that ERP system access forms were no longer required since ERP system access transitioned to being based on employee job title
- The ERP policy has not been updated to reflect current practices

Effect:

- Confidential data may have been breached
- Errors and omissions were more likely to occur

Recommendations

- The process for granting user access should be reviewed in conjunction with the current ERP Corporate policy
- Current practices and the policy should be brought into alignment

Management Agreement	Owner	Target Completion Date
Yes	Chief Safety, Security, & Technology Office	June 1, 2018

ERP Policy will be updated to reflect the current form of control. Positions in ERP will be reviewed to ensure appropriate levels are assigned and enforced.

Final Status	Medium

Implemented:
Management revised the ERP Policy to align with current practice of assigning ERP roles to users based on job title.

Management self-identified two areas of potential risk:

- The process of requesting and creating exception roles in ERP was not designed with clear roles, responsibilities, or delegations of authority [redacted]

APPENDIX 1

- [redacted]

The quarterly security review performed by super users was regarded as a mitigating control to the lack of a clearly designed process for reviewing and approving the access of new users in the ERP as well as for adjusting existing access. [redacted]

Inspection of the quarterly security report related to the mitigating control revealed:

- 1 ERP user on the Q2 and Q3 2019 Security Access Report for Accounting had left UTA more than 1 year prior
- [redacted]
- [redacted]

[redacted]

- [redacted]
- ERP Tech Sys Admin- Accounting had access to P07230 Print Payments which does not appear to be consistent with the job responsibilities of initiating payroll payments

[redacted]

- [redacted]
- [redacted]

Recommendations:

- Application Support should communicate to owners of ERP modules what they are responsible for including those activities that may be perceived to have been delegated to the super users they supervise
- Management should define how exception roles should be requested [redacted] for ERP
- Management should consider how departmental ERP super users are managed as departmental management may not have the skill and training to adequately oversee their activities. Management should consider establishing minimum levels of ongoing training and certification for ERP super users

Management Agreement	Owner	Target Completion Date
Yes	IT Director	December 31, 2020
Responses to new recommendations (from Final Status – Feb 24, 2020):		

APPENDIX 1

1. Application Support should communicate to owners of ERP modules what they are responsible for including those activities that may be perceived to have been delegated to the super users they supervise
    a. Since the time of the audit, the 11.1.1 JDE SOP has been updated to better define the roles of the super-user and authorization from the Super Users Executive (Section C. 2-4). To address the new recommendations in the final status from IA, the SOP could be further updated to have the ERP Superuser acknowledge in writing the scope and impact of their associated Superuser responsibilities
2. Management should define how exception roles should be requested and approved for ERP
    a. Currently, a Super User creates a JDE Security Change Request in POB. This ticket is reviewed by a JDE Developer and processed
        i. This is already addressed by 11.1.1 JDE SOP, Sections C.3, C.4, and C.7
3. Management should consider how departmental ERP super users are managed as departmental management may not have the skill and training to adequately oversee their activities. Management should consider establishing minimum levels of ongoing training and certification for ERP super users
    a. ERP super users and the relevant departmental management (Finance, Procurement, HR, and OAS) will collaborate with the IT Department to develop ongoing training plans to meet the individual needs of the ERP super users.

6. Bargaining Unit Employee Timekeeping

Preliminary Finding R-18-1-6	High

Criteria:

- Enterprise governance is an overarching system, which seeks to align priorities, funding, and resources and elevates decision-making responsibility, authority, and accountability to the appropriate levels. Governance principles include:
    - Management establishes reporting lines, with board oversight, of the development and performance of internal control
    - Individual accountability is in place for internal control responsibilities that support entity objectives
- COSO Framework stipulates control activities should be deployed through policies that establish what is expected and procedures that put policies into action

Sources:
COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes, Robert R Moeller
COSO: How the COSO Frameworks Can Help, James DeLoach and Jeff Thomson

Condition:

- The majority of UTA staff, approximately 1,125 Bargaining Unit operations employees, used a customized application (OWATS) to track employee time. Around 340 Bargaining Unit maintenance staff used a different timekeeping application (TC-1), which was developed by a third party. IA noted that:
    - Bargaining Unit timecard approvals were not adequate:
        - [redacted]

APPENDIX 1

    [redacted]
    - [redacted]
    - [redacted]
  - A completed timecard was not always available prior to payroll processing. Bargaining Unit employees may work up until midnight on Saturday when Payroll requests timecards on Friday due to a holiday. There were no procedures for handling lack of timecards
  - Timecards were not adequately protected from unauthorized changes, including:
    - [redacted]
    - [redacted]
    - Changes could be made to OWATS timecards at any time after they were approved, even after records were processed in ERP
    - There was no control in place in either OWATS or TC-1 to detect changes, nor a requirement that changes be reviewed and approved
  - SLBU Office Specialists did not retain OWATS timekeeping reports to support their communication to Payroll that the business unit timecards payroll process was complete
  - [redacted]
- [redacted]

Root/Cause Analysis:

- Payroll processes, roles and responsibilities have developed over time, as business needs arose
- Collective Bargaining Agreement rules and the nature of work performed may have fostered the development of satellite timekeeping system and manual timecards
- Management relied on the expertise of existing staff rather than oversight in the form of written governance or oversight
- Turn-over in key personnel

Effect:

- Dispatch supervisors and office specialists had the ability to change employee leave pay codes without review or approval by the impacted employee, an employee's supervisor, or other party
- Employees may have been under or over paid and pay disputes may be more likely to occur
- Confidential data may have been breached
- Errors and omissions were more likely to occur

Recommendations

Standard operating procedures should be reviewed and updated to include:

- Review and approval of Bargaining Unit OWATS and TC-1 employee timecards by a supervisor

APPENDIX 1

- A process to ensure that employee leave balances are reviewed prior to timecard approval and that the review is documented
- Controls to prevent undetected changes to timecards after they have been processed by Payroll
- Where changes to timecards are required, requirements that they be approved by an independent party with sufficient authority or, alternatively, implementation of a mitigating control, such as review of management reports
- Procedures for handling lack of timecards
- Required retention periods for payroll documentation, including electronic communication
- Guidelines regarding types of data stored and ongoing data reviews
- User access controls that support the approved procedures
- Segregation of duties over entering or modifying time and receipt of checks

Management Agreement	Owner	Target Completion Date
Yes	Executive Director	September 30, 2018

We will organize a group to address each of the conditions in the report to eliminate or mitigate the identified risks. We will find best practices and update needed policies and procedures to accomplish this objective. We will work toward completion of this project by end of third quarter, 2018.

Final Status	**High**

Implemented:

Draft SOPs included the following:

- Review and approval of OWATS and TC-1 timecards by business unit designees
- Requirement for review of Leave Balance Reports prior to timecard approval
- Reports and information to be retained as well as retention periods for payroll documentation
- User access controls that support the approved procedures
- Additionally, it was noted that the OWATS system restricted changes to data once it was forwarded to Payroll

Adequate segregation of duties were not designed for timekeeping roles and responsibilities which resulted in an elevated risk of inaccurate, invalid, and incorrect payment. Gaps in control design included the following:

- For many business units a blanket assignment of critical aspects of timekeeping had been assigned to the same users including preparing, reviewing, and approving timekeeping as well as review of timekeeping exceptions
- Some business units had also assigned the overall review responsibility to the same users who perform the preparation, proofing, and approval of timekeeping
- Office Admin/Specialists/Coordinators as well as supervisors that were responsible for adding and editing time in OWATS, TC-1, as well as for preparing payroll memos for interim checks, [redacted]

OWATS

Audit procedures revealed the following areas of risk for OWATS:

- [redacted]

APPENDIX 1

- The OWATS SOP requirement to run the Time Grid Extract and send it to the Operations Supervisor [redacted] For 3 of the Business Units subsampled, none of the Time Extract Grids were distributed or retained in line with the OWATS SOP
- [redacted]
- Manager reviews were intended to take place after timekeeping has been submitted but it was not clearly documented how timely or thorough the review need be nor what accountability is assigned as a result of their review

Testing of leave overage reports revealed:

- For 1 (of 2) employees who appeared on the Leave Overage Report, uncorrected vacation control entries in OWATs caused a leave overage balance
- 1 (of 2) employee subsampled the employee's vacation hours were approved even though the employee did not have vacation hours available, which should have been identified in a review of the department's Leave Balance Report

Inspection and review of the UTA wide OWATS operating procedures revealed:

- The OWATS SOP was considered in draft as of the beginning of field work and had not yet been reviewed or approved by management or implemented into operation
- The appropriate authority level and approval requirement for payroll corrections to OWATS was not defined
- [redacted]
- The treatment of a lack of timecards and for timekeeping approval not performed was not defined, resulting in the risk that paychecks are issued incorrectly or invalidly
- [redacted]

TC-1

Audit procedures revealed the following areas of risk for TC-1:

- Facilities Maintenance personnel might clock in at any time before their shift, in some cases hours beforehand, without compensation
- It is not clear that Facilities Maintenance personnel agreed to the hours paid as scheduled and gave up a claim to hours as punched on the signed off timecard
- There was no review of payroll processed to confirm that it matched the timekeeping approved and to ensure it was not changed in the period between approval and locking the system to changes
- In the period between when a Facilities Maintenance Supervisor had informed the Maintenance System ERP Admin that their process was complete until all had done so and the system could be locked, changes could have been made and not caught before payroll was processed
- The lack of an approved timecard was not addressed in the SOP, resulting in the risk that paychecks may have been issued incorrectly or invalidly

APPENDIX 1

- It was also noted that the Facilities Maintenance department identified the Maintenance System ERP as responsible for ensuring time record accuracy which did not align with his responsibilities and per inquiry with him he did not perform
- [redacted]
- TC-1 SOP required that supervisors email communication of their completed review to the Maintenance System ERP Admin, however, testing of TC-1 timekeeping in practice revealed that no evidence of communication of supervisor review could be identified for the 7 supervisors selected for the two pay periods tested

Inspection and review of the UTA wide TC-1 SOP revealed the following:

- The SOP was in draft as of the beginning of field work and had not yet been reviewed or approved by management or implemented into operation
- The SOP did state that responsibilities are to be separated, however, it did not indicate which responsibilities required segregation e.g. the office specialist adding/editing time and receiving paychecks

Manual Process
Inspection and review of the UTA wide manual payroll processing SOP revealed the following:

- The policy was in draft as of the beginning of field work and had not yet been approved by Management
- It did not address how Payroll Administrators had to proceed when the timecards were not received for all employees

Recommendations:

- Management should consult with legal advisors to assess the risk of allowing employees to clock-in in advance of a shift and decide whether employees punching in at any time other than when they are starting or continuing a shift is appropriate. The practice of allowing employees to clock in for an extended period of time (<15 min+) before they begin working may put UTA at risk of owing back pay regardless of the original intent of the early punch in
- [redacted]
- Management should separate duties within the timekeeping and reporting process to assure that authorization, recording, and custody responsibilities are adequately separated. For example, the party responsible for entering time should not be the same party who reviews and approves the timekeeping. Ideally, neither the initiator nor the approver of timekeeping should take custody of a paper checks. Likewise, the duties of interim check request, approval, and custody should also be separated
- When an approved timecard is not available Management should define in an SOP what is necessary for paying an employee without an approved timecard
- OWATS timekeeping reviewers should include vacation control entries as part of their overall review of timekeeping
- Management should review departmental payroll activity from the ERP against timekeeping submitted to confirm that the timekeeping was the basis for the payroll as well as to identify any unusual or unexpected items

APPENDIX 1

- All timekeeping review processes should include confirmation that any paid leave requested is supported by the current Leave Balance Report
- [redacted]
- Management should finalize the timekeeping system specific SOPs and define how often they will be reviewed and approved

Management Agreement	Owner	Target Completion Date
Yes	Chief Operating Officer	December 31, 2020

Operations management agrees with the audit results and will take the necessary steps to mitigate risks to the greatest extent possible. Operations' management will work with other related departments to develop a work group to standardize processes and put necessary controls in place to mitigate the identified risks. Responses to recommendations are as follows:

- Employees have been instructed on clock-in procedures. Employees will not clock-in more than 15 minutes prior to schedule shift unless otherwise approved by their supervisor. Supervisors will audit clock-in times when completing bi-weekly timekeeping and coach/discipline as necessary. Additionally, we will develop a process to add a disclaimer to the timesheet explaining to employees that they are signing for the hours they worked and will be paid only for the hours signed for
- The IT department has created a report, which will be automatically generated at when OWATS passes to JDE, which reports pay codes from both systems. This report will be electronically sent to the person auditing payroll, Assistant Operations Manager, Manager and RGM for review prior to the end of the next pay period.
- Accounting Process – Accounting is currently working to develop a process to approve payment without an approved time card
- Operations management agrees and will confirm this expectation in regards to vacation control
- Operations management agrees to review OWATS reports as outlined in the SOP
- Operations management agrees with this recommendation for TC1. However, OWATS is the control system used unless we are auditing for sell back vacation. OWATS is the keeper of the data and is reflective of the information contained of the recommended reports.
- On a monthly basis, Payroll will provide the Operations Service Unit General Managers/RGM's a report of all interim payments made to departmental employees.
- SOPs have been created and in place
- Operations management agrees with this recommendation and will ensure appropriate personnel are responsible for timekeeping accuracy as outlined in the SOP

APPENDIX 1

7. Bargaining Unit Employee Timekeeping Application Administration

Preliminary Finding R-18-1-7	High

Criteria:

- Enterprise governance is an overarching system, which seeks to align priorities, funding, and resources and elevates decision-making responsibility, authority, and accountability to the appropriate levels. Governance principles include:
  - Management establishes reporting lines, with board oversight, of the development and performance of internal control
  - Individual accountability is in place for internal control responsibilities that support entity objectives
- COSO Framework stipulates control activities should be deployed through policies that establish what is expected and procedures that put policies into action

Sources:
COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes, Robert R Moeller
COSO: How the COSO Frameworks Can Help, James DeLoach and Jeff Thomson

Condition:

Data generated from both Bargaining Unit OWATS and TC-1 systems was uploaded each pay period into ERP for payroll processing. The timekeeping systems were administered by Operations and Analysis division employees. IA noted that:

- TC-1 used by Bargaining Unit maintenance employees was no longer supported by the vendor
- IA found that access controls for both timekeeping systems were not adequate, based on the following:
  - There was no formal process for requesting, reviewing and approving new users or changes to user security levels
  - There was no routine, periodic review of employee access levels nor standard operating procedures regarding access controls
  - 112 (out of 373) OWATS users had the ability to create or change timekeeping data, although they did not appear to have clear timekeeping authority or responsibility
  - Users had excessive levels of access to TC-1:
    - IA noted that 4 out of 7 TC-1 users that were listed as supervisors, had excessive, administrative-levels access
    - 2 of the 4 users did not supervise employees, including an office specialist and a maintenance training administrator
    - With 1 exception, supervisor accounts sampled had supervisory access rights that exceeded the number of employees they supervised per the phone directory
  - Access for employees that had terminated or transferred departments was not always revoked or disabled
    - IA noted 22 former employees out of 373 users with access to OWATS timecards
    - While testing TC-1 supervisory access levels, IA observed 2 active employee user accounts for employees that left the employment of UTA
  - TC-1 system user logins and passwords were both set to the employee's badge number
  - There was no requirement to change assigned passwords
- Change management controls were not adequate, including:

APPENDIX 1

  - There was no test environment for implementing Collective Bargaining Agreement or other business rules in TC-1
  - Although there was a test environment for making business rules and other changes to OWATS, there was no SOP or policy to govern how changes should be requested, tracked, tested, approved, or moved into production
  - Individual authority to request, implement, review and approve changes was not in place
  - IT change control procedures, requiring application changes to be reviewed by the Technology Change Control Board prior to implementation, were not followed for the intermediary application that was used to convert bargaining unit systems timecodes to ERP timecodes
  - There was no periodic monitoring of timecode conversion accuracy from the Bargaining Unit systems timecodes to ERP timecodes
  - There were no periodic reviews of user access by the process owner to the intermediary application or network drive where bargaining unit timecard data was stored prior to conversion

Root/Cause Analysis:

- Payroll processes, and roles and responsibilities have developed over time, as business needs arose
- Collective Bargaining Agreement rules and the nature of work performed may have fostered the development of satellite timekeeping system and manual timecards
- Management relied on the expertise of existing staff rather than oversight in the form of written governance or oversight
- Turn-over in key personnel

Effect:

- Staff may be over or under paid
- Timekeeping records may not agree, resulting in pay disputes
- Errors and omissions are more likely to occur
- The risk of invalid or fraudulent entries is increased
- Unsupported software may result in interruption of payroll processes in the event that software stops functioning correctly

Recommendations

Standard operating procedures should be developed and implemented that include:

- A formal process for requesting, reviewing and approving new users or changes to user security levels for timekeeping systems
- Monitoring of existing user accounts for appropriate access levels
- Deactivating or removing accounts for users who no longer need access due to termination, department transfer, or other change in job duties
- Requirements for unique logins and passwords, known only to the user
- Change management controls, including authorizing, tracking, testing, approving and migrating changes into production within the timekeeping system and intermediary application
- Monitoring of timecode conversion accuracy and periodic reviews of user access to the intermediary application and data

APPENDIX 1

Management Agreement	Owner	Target Completion Date
Yes	Chief Safety, Security, & Technology Office	September 1, 2018

A Standard Operating Procedure (SOP) will be created for Operations and Maintenance timekeeping for Payroll processing. This SOP will address all Payroll related timekeeping system controls (ERP, TC-1, and OWATS). The SOP will establish a formal process to address the following:

- Requesting, reviewing and approving new users or changes to user security levels for timekeeping systems
- Monitoring of existing user accounts for appropriate access levels once a quarter starting by September 3, 2018
- Deactivating or removing accounts for users who no longer need access due to termination, department transfer, or other change in job duties as per HR notification and already established Human Resource Action Form (HRAF) notification
- Requirements for unique logins and passwords, known only to the user, by utilizing already in place, Active Directory network user authentication
- For Accounting Department to request changes, communicate requirements, and approve final testing
- Following TCCB (Technology Change Control Board) process for all Payroll changes (to include adding or changing conversion pay codes and programming changes for rules, etc.). This will include authorizing, tracking, testing, approving and migrating changes from development into production within the timekeeping system and intermediary ERP timesheet import application

Follow the Payroll SOP (to be written), to monitor timecode conversion accuracy and periodic reviews of user access to the intermediary application and data.

Final Status	High

Implemented:
SOP requirements included assigning ownership of review and approval of timekeeping application user accounts as well as the responsibility to periodically review access to systems to the Senior Accountant over Payroll. Additionally, change management controls were documented in the Payroll SOP including assignment of approval of changes to the Senior Accountant over Payroll and the requirement for changes to follow the Technology Change Control Board process.

[redacted]

OWATS

[redacted]

- [redacted]
- [redacted]

APPENDIX 1

- [redacted]

Testing of OWATS Admin user accounts revealed:

- [redacted]
- [redacted]

TC-1
Testing of TC-1 user accounts revealed:

- [redacted]
- [redacted]
- Access accounts in TC-1, [redacted], had the ability to make editable changes that had unknown potential effects on timekeeping but could result in inability to complete timekeeping conversion or incorrect pay codes applied to employee time

Recommendations:

- After owners for the timekeeping systems have been identified (see Finding 1) they should assign the role and related responsibilities of administering the system
- [redacted]
- [redacted]
- [redacted]
- A timekeeping system administrator(s) should monitor timecode conversion accuracy for the intermediary application and data

Management Agreement	Owner	Target Completion Date
Yes	Chief Operating Officer	December 31, 2020

Operations management agrees with the audit results and will take the necessary steps to mitigate risks to the greatest extent possible. Operations management will work with other related departments to develop a work group to standardize processes and put necessary controls in place to mitigate the identified risks. Responses to recommendations are as follows:

- The COO is the OWATS owner and will assign roles and responsibilities appropriately in coordination with Accounting and OAS
- This finding been corrected. Access is limited appropriately as only those with a legitimate business purpose have the ability to view sensitive Operator information

APPENDIX 1

- The Chief Operating Officer is the owner of OWATS and will appoint an individual to review appropriateness of access
- This item is complete. The assigned timekeeping administrator ensures the system requirements include unique logins and passwords, only known by the user. This was completed the latest OWATS upgrade
- Accounting Process –OAS and Accounting will work together to resolve any discrepancies

APPENDIX 2

RATING MATRIX

DETAILED FINDING PRIORITY RATING

Descriptor	Guide
High	Matters considered being fundamental to the maintenance of internal control or good corporate governance. These matters should be subject to agreed remedial action within three months.
Medium	Matters considered being important to the maintenance of internal control or good corporate governance. These matters should be subject to agreed remedial action within six months.
Low	Matters considered being of minor importance to the maintenance of internal control or good corporate governance or that represents an opportunity for improving the efficiency of existing processes. These matters should be subject to agreed remedial action and further evaluation within twelve months.
Implemented	Management action has been taken to address the risk(s) noted in the audit finding.

APPENDIX 3

DISTRIBUTION LIST

Name	For Action[1]	For Information	Reviewed prior to release
Executive Director			*
Chief Financial Officer	*		*
Chief People Officer	*		*
Chief Operating Officer	*		*
Comptroller	*		*
IT Director	*		*
Senior Manager Operations Analysis & Solutions	*		*
Senior Accountant	*		*
Payroll Administrators	*		*
Director of HR Services and Labor Relations	*		*
Manager Total Rewards	*		*
HRIS – Technology System Admin	*		*
Manager of Operations Maintenance Systems Architecture & Solutions	*		*

[1] For Action indicates that a person is responsible, either directly or indirectly depending on their role in the process, for addressing an audit finding.