HUMAN RESOURCES PAYROLL CONTROLS ASSURANCE ENGAGEMENT

Report No. AE-2024-2

JUNE 3, 2024

Utah County Auditor Internal Audit Division
Internal Audit Manager: Calvin Bergmann, CIA, MPA
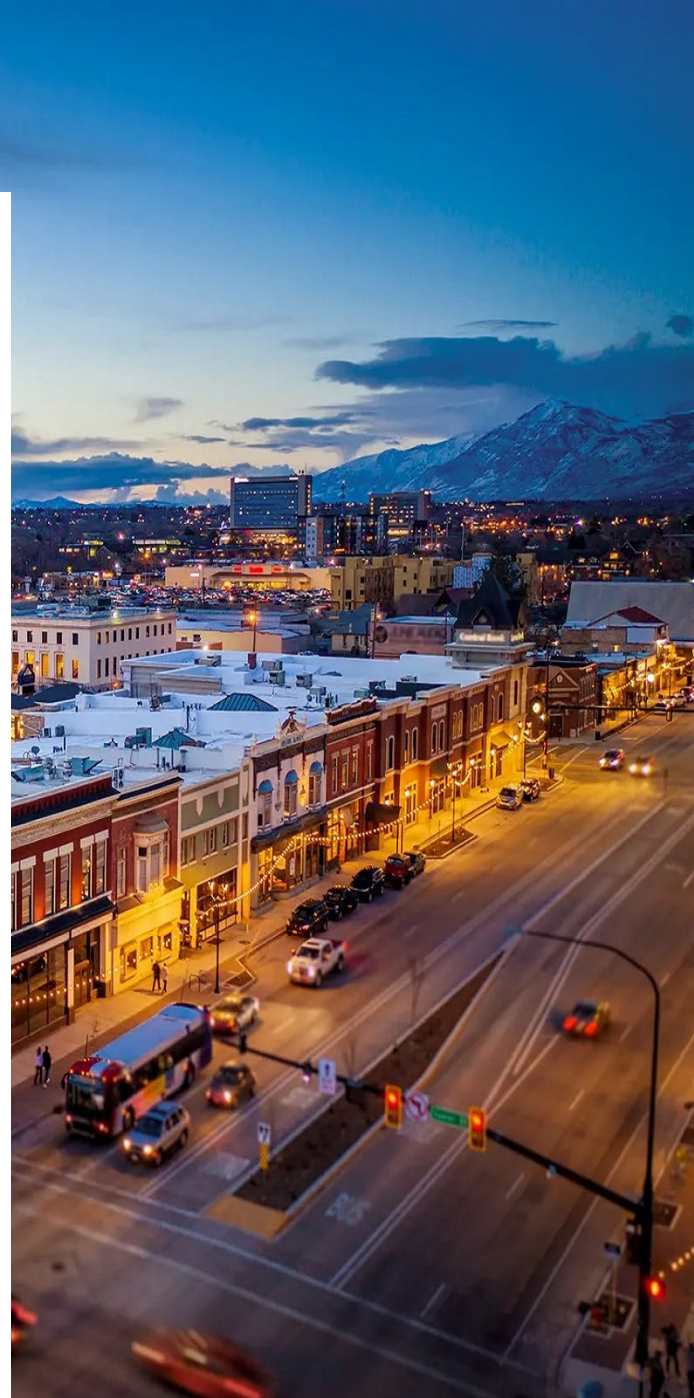**Senior Internal Auditor: Mont Wade, CIA**

Utah County
HEART *of* UTAH

TABLE OF CONTENTS

AUDITOR'S LETTER

Office of the County Auditor
Internal Audit Division

June 3, 2024

Ralf Barnes, Director
Utah County Office of Human Resource Management
100 East University Avenue
Provo, Utah 84606

Dear Mr. Barnes:

The Internal Audit Division ("Division") performed an assurance engagement of Human Resources payroll controls. During this limited review, we performed the following procedures:

1. For calendar year 2024, tested Workday payroll control separation of duties for Human Resources employee population comprising:
   a. Run Manual Payment for Worker
   b. Run On Demand Payment for Worker
   c. Run Pay Calculation
   d. Run Pay Complete
   e. INT019 Payroll ACH Out (i.e., generate bank ACH file)
   f. Change Account Information
   g. Add Account
   h. Hiring
      i. Create Position
      ii. Change Organization Assignments for Worker
      iii. Hire (Create Pre-Hire)
      iv. Propose Compensation Hire
      v. Change Organization Assignments
      vi. Edit Additional Data
   i. One-Time Payment
   j. Request Compensation Change

  k. Enter Time (i.e., enter an employee's time other than the HR employee's personal time)
2. For calendar year 2023, tested 20 compensation changes for operating procedure recording and authorization compliance.

The Division discovered fourteen findings and four other matters during the engagement. For both findings and other matters, we provide recommendations to improve Human Resource's payroll control environment. Finding and other matter numbering is correlated with the procedures listed above.

Note that our report, by nature, disproportionately focuses on weaknesses. This does not mean there were not strengths within the areas reviewed and other areas not reviewed.

The Division appreciates the courtesy and assistance extended to us by Utah County Human Resources personnel during the engagement process. We look forward to a continuing professional relationship.

Sincerely,

Utah County Internal Audit Division

CC: Rodney Mann, Utah County Auditor, Utah County Audit Committee Chair
  Amelia Powers Gardner, Utah County Commissioner

FINDING(S) & OTHER MATTER(S)

Finding 1.1: Insufficient Payroll System Separation of Duties (Payroll Processing and Change Bank Account Information)

Condition

Seven Human Resources employees can execute the "Change Account Information" process and "Add Account" process. When the "Change Account Information" process is executed, Workday reports a "completed" status and it appears that no further action is necessary. When the "Add Account" process is executed, no status is reported on the "Payment Elections" page, but the new account appears on the "Payment Elections" page, and it appears that no further action is necessary.

Five of these seven employees can also execute the "Run Pay Calculation" process, "Run Pay Complete" process, and "INT019 Payroll ACH out" process.

Two of these seven employees can also execute the "INT019 Payroll ACH out" process.

Human Resources employees can execute both payroll processes (i.e., initiating payroll, approving payroll, and creating the ACH bank payroll file) and a bank account information editing process (i.e., editing bank account data for employees other than themselves).

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Change Account Information" process and/or the "Add Account" process cannot execute payroll processing processes. We further recommend that the "Change Account Information" process and "Add Account" process be eliminated from all Human Resource employee role-based security and user-based security profiles (ensuring Human Resource employees retain the permission to edit their personal bank account information), and that new employees, as a condition of employment, be required to enter their own bank account information before they begin employment or during an onboarding process on the new employee's first day of work.

Finding 1.2: Insufficient Payroll Control Separation of Duties (Payroll Processing and Hiring)

Condition

Six Human Resources employees can execute comprehensive hiring processes (i.e., "Create Position," "Change Organization Assignments for Worker," "Hire (Create Pre-Hire)," "Propose Compensation Hire," "Change Organization Assignments," and "Edit Additional Data" processes).

Four of these six employees can also execute the "Run Pay Calculation" process, "Run Pay Complete" process, and "INT019 Payroll ACH out" process.

One of these six employees can also execute the "INT019 Payroll ACH out" process.

Human Resources employees can execute both payroll processes (i.e., initiating payroll, approving payroll, and creating the ACH bank payroll file) and hiring processes.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties...applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute hiring processes cannot execute payroll processing processes.

Finding 1.3: Insufficient Payroll System Separation of Duties (Payroll Processing and One-Time Payment)

Condition

Thirteen Human Resources employees can execute the "Request One-Time Payment" process. When the "Request One-Time Payment" step is executed, Workday reports a "step completed" status and it appears that no further action is necessary.

Five of these thirteen employees can also execute the "Run Pay Calculation" process, "Run Pay Complete" process, and "INT019 Payroll ACH out" process.

Two of these thirteen employees can also execute the "INT019 Payroll ACH out" process.

Human Resources employees can execute both payroll processes (i.e., initiating payroll, approving payroll, and creating the ACH bank payroll file) and execute a one-time payment process.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Request One-Time Payment" process cannot execute payroll processing processes. We further recommend that the "Request One-Time Payment" process, when executed (i.e., processed and recorded) by a Human Resources employee, require a second Human Resources employee to verify (i.e., authorize) the data recorded.

Finding 1.4: Insufficient Payroll System Separation of Duties (Payroll Processing and Change Compensation)

Condition

Eleven Human Resources employees can execute the "Request Compensation Change" process. When the "Request Compensation Change" step is executed, Workday reports a "completed" status and it appears that no further action is necessary.

Five of these eleven employees can also execute the "Run Pay Calculation" process, "Run Pay Complete" process, and "INT019 Payroll ACH out" process.

Two of these eleven employees can also execute the "INT019 Payroll ACH out" process.

Human Resources employees can execute both payroll processes (i.e., initiating payroll, approving payroll, and creating the ACH bank payroll file) and a compensation change process.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Request Compensation Change" process cannot execute payroll processing processes.

Finding 1.5: Insufficient Payroll System Separation of Duties (Payroll Processing and Time Entry)

Condition

Seven Human Resources employees can execute the "Enter Time" process. When the "Enter Time" step is executed, Workday reports a "not required" status for the "Approval by Manager or Timekeeper" step and "To Do: Timekeeper Time Entry" step.

Five of these seven employees can also execute the "Run Pay Calculation" process, "Run Pay Complete" process, and "INT019 Payroll ACH out" process.

Two of these seven employees can also execute the "INT019 Payroll ACH out" process.

Human Resources employees can execute both payroll processes (i.e., initiating payroll, approving payroll, and creating the ACH bank payroll file) and a timekeeping process (i.e., entering time for employees other than themselves).

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties...applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Timesheet fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Enter Time" process cannot execute payroll processing processes. We further recommend that the "Enter Time" process, when executed (i.e., processed and recorded) by a Human Resources employee for other County employees, require a second Human Resources employee to verify (i.e., authorize) the data recorded.

Finding 1.6: Insufficient Payroll System Separation of Duties (Calculate Payroll and Complete Payroll)

Condition

Five Human Resources employees can execute the "Run Pay Calculation" process.

Five of these five employees can also execute the "Run Pay Complete" process.

Human Resources employees can both calculate payroll and complete payroll.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Run Pay Calculation" process cannot execute the "Run Pay Complete" process.

Finding 1.7: Insufficient Payroll System Separation of Duties (Calculate Payroll and Output Bank File)

Condition

Five Human Resources employees can execute the "Run Pay Calculation" process.

Five of these five employees can also execute the "INT019 Payroll ACH out" process.

Human Resources employees can both calculate payroll and output the ACH bank file.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties...applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Run Pay Calculate" process cannot execute the "INT019 Payroll ACH out" process.

Finding 1.8: Insufficient Payroll System Separation of Duties (Complete Payroll and Output Bank File)

Condition

Five Human Resources employees can execute the "Run Pay Complete" process.

Five of these five employees can also execute the "INT019 Payroll ACH out" process.

Human Resources employees can both complete payroll and output the ACH bank file.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Run Pay Complete" process cannot execute the "INT019 Payroll ACH out" process.

Finding 1.9: Insufficient Payroll System Separation of Duties (Payroll Adjustments and Change Bank Account Information)

Condition

Six Human Resources employees can execute the "Run Manual Payment for Worker" process and "Run On Demand Payment for Worker" process.

Six of these six employees can also execute the "Change Account Information" process and "Add Account" process.

Human Resources employees can both enter payroll adjustments and change bank account information.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Run Manual Payment for Worker" process and/or the "Run On Demand Payment for Worker" process cannot execute the "Change Account Information" process and "Add Account" process.

Finding 1.10: Insufficient Payroll System Separation of Duties (Payroll Adjustments and Hiring)

Condition

Six Human Resources employees can execute the "Run Manual Payment for Worker" process and "Run On Demand Payment for Worker" process.

Five of these six employees can also execute comprehensive hiring processes (i.e., "Create Position," "Change Organization Assignments for Worker," "Hire (Create Pre-Hire)," "Propose Compensation Hire," "Change Organization Assignments," and "Edit Additional Data" processes).

Human Resources employees can both enter payroll adjustments and complete hiring processes.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Run Manual Payment for Worker" process and/or the "Run On Demand Payment for Worker" process cannot execute hiring processes.

Finding 1.11: Insufficient Payroll System Separation of Duties (Change Bank Account Information and Hiring)

Condition

Seven Human Resources employees can execute the "Change Account Information" process and "Add Account" process.

Five of these seven employees can also execute comprehensive hiring processes (i.e., "Create Position," "Change Organization Assignments for Worker," "Hire (Create Pre-Hire)," "Propose Compensation Hire," "Change Organization Assignments," and "Edit Additional Data" processes).

Human Resources employees can both change bank account information and complete hiring processes.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure that Human Resources employees who can execute the "Change Account Information" process and "Add Account" process cannot execute hiring processes.

Finding 1.12: Insufficient Payroll System Separation of Duties (IS Employee Compensation Partner Role-Based Security Profile)

Condition

Acknowledging that we specifically tested Human Resources employee payroll system permissions within a Workday sandbox environment (which management communicated is weekly refreshed based upon the production environment), we noted an Information Systems employee has a "Compensation Partner" role-based security profile.

Criteria

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizati*ons (emphasis added): "Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes *dividing mission or business functions and support functions* among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties."

In effect, programmers should have access only to development environments. They should never have the ability to modify live data or access a production environment where data is stored and processed.

Per the National Institute of Standards and Technology's (i.e., "NIST's") *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*: "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties…applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud and decreased data integrity have an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management ensure all Information Systems employees have role-based and user-based security profiles restricted to solely read-only access within the Workday production environment. Ideally, we recommend management restrict Information Systems employees entirely from accessing the Workday production environment.

Finding 1.13: Insufficient Payroll System Separation of Duties (Process Execution Recording and Authorization)

Condition

While we primarily tested Human Resources employee payroll system permissions in relation to each other and in relation to entire financial transactions, we also noted individual processes were initiated and automatically completed (i.e., "Status: Completed," Status: Step Completed," or "Status: Submitted") without a second employee authorizing the process to be executed. For example, "Run Manual Payment for Worker," "Run On Demand Payment for Worker," "Create Position," "Change Organization Assignments for Worker," "Hire Employee," "Propose Compensation Hire," "Change Organization Assignments," "Edit Additional Data," "Request One-Time Payment," "Request Compensation Change," "Change Account Information," "Add Account," and "Enter Time" processes were all executed by an individual employee.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event."

Cause

Previous Human Resources management rapidly implemented Workday and did not critically consider appropriate role-based and user-based security internal controls. Current management has not been compelled to comprehensively design, monitor, and enforce appropriate Workday role-based and user-based security internal controls.

Effect

Payroll fraud has an increased likelihood of occurrence. Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management configure Workday to ensure each process (i.e., process step) is recorded by one employee and finalized by a second, different employee.

Finding 2.1: Nonexistent Compensation Change Standard Operating Procedures

Condition

While testing a sample of compensation changes for recording and authorization in accordance with standard operating procedures (i.e., "SOPs"), management informed us that compensation change SOPs do not exist.

Criteria

Per the United States Government Accountability Office's ("GAO's") *Standards for Internal Controls in the Federal Government*: "Management should implement control activities through policies."

Cause

Current management has not been compelled to draft and enforce comprehensive Workday compensation change procedures.

Effect

Management does not have reasonable assurance that entity objectives (e.g., effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations) will be achieved.

Recommendation

We recommend management draft comprehensive Workday compensation change procedures. While acknowledging that payroll procedures already exist, we further recommend management draft comprehensive Workday procedures for all processes, including which job titles perform which duties (i.e., delineate the "who," "what," "where," "when," and "why"). This provides accountability, reduces error, and will help ensure institutional knowledge is not lost when employees leave County employment (as well as ensure current employees do not understand procedures differently than one another). This also provides a basis by which Information Systems employees and/or contractors can compare their design of Workday (or future system) internal controls.

Other Matter 1.1: Unrestricted Incompatible Compensation Grade and Job Profile Submission

Condition

While testing the "Request Compensation Change" process, we noted the "Total Base Pay Range" can be changed to a compensation grade that does not match the employee's job profile. When selecting the "Submit" button, an alert message is produced, which states "The compensation grade for this worker does not match the compensation grade from the job profile. The job profile returned a different value than what is being selected for this compensation process." After exiting the "Alert" window and selecting the "Submit" button a second time, the "Request Compensation Change" process is successfully completed (i.e. "Status: Step Completed").

Recommendation

We recommend management configure Workday to prevent compensation grades from being assigned to employees with job profiles that do not include the compensation grade within their profile compensation grade range.

Other Matter 1.2: Nonexistent One-Time Payment Threshold

Condition

While testing the "One-Time Payment" process, we noted any value can be entered and executed. For example, we changed an employee's one-time payment to $500,000, $5,000,000, $5,000,000,000, and $5,000,000,000,000 values during separate "One-Time Payment" processes. The One-Time Payment process was successfully executed in all cases. We further noted on the "Details and Process" page that "Target Amount," "Recommended Minimum," and "Recommended Maximum" values were each set to "0.00."

Recommendation

We recommend management configure Workday to ensure One-Time Payments are restricted to reasonable thresholds.

Other Matter 1.3: Unmasked Sensitive Employee Data

Condition

While testing the "Change Account Information" process and "Add Account" process, we noted that bank account numbers were displayed in their entirety on the "Change Account Information" page and "Add Account" page. We acknowledge that on the "Payment Elections" page, only the bank account number's last four digits were displayed, with six asterisks preceding the account number's last four digits. We further noted that on the employee "Personal" "IDs" page, the employee Social Security Number is displayed in its entirety.

Recommendation

We recommend management configure Workday to mask sensitive data, including bank account numbers and Social Security Numbers.

Other Matter 1.4: Unregulated Out-of-State Worker Locations

Condition

While testing the "Create a Position" process, we noted that the worker location had options for Arkansas and Idaho. We are not aware of any Human Resources policy that explicitly allows, disallows, or regulates employees working outside the State of Utah. However, we acknowledge that *Utah County Government Human Resources Policy 2-1700: Telecommuting*, states: "The employee's primary home residence workspace will be the only workspace considered an extension of the County's on-site workspace. Telecommuting from any other location is not authorized except as specifically directed by the department head in exigent circumstances."

Recommendation

We recommend management clearly define whether locations outside the State of Utah (e.g., specific states, countries, etc.) are permitted as a worker location and under what conditions these locations are permitted (e.g., authorization, duration, adequate supervision, performance standards, information security, etc.). We further recommend management establish procedures to comply with local, state, and country tax law, as well as locality-specific employment law.

MANAGEMENT RESPONSE(S)

Finding 1.1: Insufficient Payroll System Separation of Duties (Payroll Processing and Change Bank Account Information)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Change Account Information" process and/or the "Add Account" process cannot execute payroll processing processes. We further recommend that the "Change Account Information" process and "Add Account" process be eliminated from all Human Resource employee role-based security and user-based security profiles (ensuring Human Resource employees retain the permission to edit their personal bank account information), and that new	Agree – with modification	Security group is now limited to Payroll Admin (Robin D) and Payroll Partner (Sadie R). Payroll must have access to facilitate prenote process when erroneous account numbers are provided. Business process automatically informs employee of any account changes. No other employees have access to modify another's bank account information. Mhai needs to also have security for this, and for her there will be a second approval step for add and edit (Robin D.)if not initiated by the employee.	Brandon Chambers/Benefits Manager, Robin Davis/Payroll Administrator	10/15/2024

employees, as a condition of employment, be required to enter their own bank account information before they begin employment or during an onboarding process on the new employee's first day of work.

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.2: Insufficient Payroll Control Separation of Duties (Payroll Processing and Hiring)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute hiring processes cannot execute payroll processing processes.	Agree	Payroll admin access has been removed from all HR employees other than payroll admin EE's. Recruiting employees admin EE's access to payroll removed.	Brandon Chambers/Benefits Manager, Robin Davis/Payroll Administrator,	7/19/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.3: Insufficient Payroll System Separation of Duties (Payroll Processing and One-Time Payment)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Request One-Time Payment" process cannot execute payroll processing processes. We further recommend that the "Request One-Time Payment" process, when executed (i.e., processed and recorded) by a Human Resources employee, require a second Human Resources employee to verify (i.e., authorize) the data recorded.	Agree - But one time payment is a non functional process.	Non-functional. Not usable. Has been inactivated.	Merritt Fullmer	6/27/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.4: Insufficient Payroll System Separation of Duties (Payroll Processing and Change Compensation)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Request Compensation Change" process cannot execute payroll processing processes.	Agree - Modification	No comp change/approve payroll allowed. Payroll admin group is reviewed and reduced to Robin D, Sadie. Only Mhai has access to both. Create a business process that requires a 2nd approval for any edits made by Mhai.	Brandon Chambers/Benefits Manager, Robin Davis/Payroll Administrator, Merritt Fullmer/CM	10/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.5: Insufficient Payroll System Separation of Duties (Payroll Processing and Time Entry)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Enter Time" process cannot execute payroll processing processes. We further recommend that the "Enter Time" process, when executed (i.e., processed and recorded) by a Human Resources employee for other County employees, require a second Human Resources employee to verify (i.e., authorize) the data recorded.	Agree - Modification	Functionality to edit time must be allowed in order to resolve pay issues. Corrections per policy need to happen for an employee time card if they entered in ineligible Holiday Pay, Paid Time Off, or incorrect time record. Any changes are auditable. 2nd payroll EE can verify time changes. Notifications are sent that a change has been made by TimeKeeper. Run Time change audit report to be reviewed.Will remove anyone in security groups not necessary for the function.	Robin Davis/Payroll Administrator	9/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.6: Insufficient Payroll System Separation of Duties (Calculate Payroll and Complete Payroll)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Run Pay Calculation" process cannot execute the "Run Pay Complete" process.	Agree	Payroll Admin security group will be updated to remove unnecessary individuals that have access to the task. Current internal process is to do a final audit on these pay calculations prior to pay complete. Duties are separated in Task between pay specialist and pay administrator. Approval by payroll administrator.	Robin Davis/ Payroll Admin	10/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.7: Insufficient Payroll System Separation of Duties (Calculate Payroll and Output Bank File)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Run Pay Calculate" process cannot execute the "INT019 Payroll ACH out" process.	Agree	Payroll Admin security group will be updated to remove unnecessary individuals that have access to the task. Current internal process is to do a final audit on these pay calculations prior to payroll out complete. Duties are separated in Task between pay specialist and pay admin.	Robin Davis/ Payroll Admin	10/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.8: Insufficient Payroll System Separation of Duties (Complete Payroll and Output Bank File)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Run Pay Complete" process cannot execute the "INT019 Payroll ACH out" process.	Agree	Move this function and responsibility to treasurer.	Treasuer	9/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.9: Insufficient Payroll System Separation of Duties (Payroll Adjustments and Change Bank Account Information)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Run Manual Payment for Worker" process and/or the "Run On Demand Payment for Worker" process cannot execute the **"**Change Account Information" process and "Add Account" process**.**	Agree - Modification	Only employees themselves can edit their own bank account information. Payroll team can view and edit. Second approval step for add and edit (Robin D.)if not initiated by the employee.	Brandon Chambers/Benefits Manager, Robin Davis/Payroll Administrator,	09/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.10: Insufficient Payroll System Separation of Duties (Payroll Adjustments and Hiring)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Run Manual Payment for Worker" process and/or the "Run On Demand Payment for Worker" process cannot execute hiring processes.	Agree	Hiring process security roles to be limited to recruitment staff.	Robin Davis/ Payroll Admin	07/19/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.11: Insufficient Payroll System Separation of Duties (Change Bank Account Information and Hiring)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure that Human Resources employees who can execute the "Change Account Information" process and "Add Account" process cannot execute hiring processes.	Agree	Only employees themselves can edit bank their own bank account information. Second approval step for add and edit (Robin D.)if not initiated by the employee. Payroll admin no hiring authority.	Brandon Chambers/ Benefits Manager, Robin Davis/ Payroll Administrator,	10/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.12: Insufficient Payroll System Separation of Duties (IS Employee Compensation Partner Role-Based Security Profile)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management ensure all Information Systems employees have role-based and user-based security profiles restricted to solely read-only access within the Workday production environment. Ideally, we recommend management restrict Information Systems employees entirely from accessing the Workday production environment.	Agree	IS created report shows specific process role based security. Once identified separation of processes will be implemented and modify, edit access will be removed. View access will be allowed as needed.	Payroll,Benefits & IS Team. Brandon Chambers/Benefits Manager, Robin Davis/Payroll Administrator, Ranjith/IS	9/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 1.13: Insufficient Payroll System Separation of Duties (Process Execution Recording and Authorization)

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management configure Workday to ensure each process (i.e., process step) is recorded by one employee and finalized by a second, different employee.	Agree with modification	Request limiting this recommendation to processes that represent financial risk - per previous items.	TBD	12/01/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Finding 2.1: Nonexistent Compensation Change Standard Operating Procedures

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management draft comprehensive Workday compensation change procedures. While acknowledging that payroll procedures already exist, we further recommend management draft comprehensive Workday procedures for all processes, including which job titles perform which duties (i.e., delineate the "who," "what," "where," "when," and "why"). This provides accountability, reduces error, and will help ensure institutional knowledge is not lost when employees leave County employment (as well as ensure current employees do not understand	Agree	Comp team will complete process SOP. Comp team has a comprehensive process for reviewing and auditing compensation changes outside of Workday.	Merritt Fullmer/ Comp Manager	12/15/2024

procedures differently than one another). This also provides a basis by which Information Systems employees and/or contractors can compare their design of Workday (or future system) internal controls.

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Other Matter 1.1: Unrestricted Incompatible Compensation Grade and Job Profile Submission

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management configure Workday to prevent compensation grades from being assigned to employees with job profiles that do not include the compensation grade within their profile compensation grade range.	Agree - modification	The system warns that this request is happening. Change to prohibit. Comp Admin security group to be updated (limited) for user access. Very Rare occasions have happened when a job profile needs to be paid outside their normal pay range. Will require additional approver.	Merritt Fullmer/ Comp Manager	12/1/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Other Matter 1.2: Nonexistent One-Time Payment Threshold

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management configure Workday to ensure One-Time Payments are restricted to reasonable thresholds.	Agree - but this does not function	Non-functional removed from system .	Merritt Fullmer/ Comp Manager	6/27/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Other Matter 1.3: Unmasked Sensitive Employee Data

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management configure Workday to mask sensitive data, including bank account numbers and Social Security Numbers.	Agree - Modification	Bank Account info limited to Payroll admin. Payroll needs security to view bank info with second approval step if not initiated by the employee. Benefits need view of SS #.	Ranjith/IS	10/15/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.

Other Matter 1.4: Unregulated Out-of-State Worker Locations

Management Response

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management clearly define whether locations outside the State of Utah (e.g., specific states, countries, etc.) are permitted as a worker location and under what conditions these locations are permitted (e.g., authorization, duration, adequate supervision, performance standards, information security, etc.). We further recommend management establish procedures to comply with local, state, and country tax law, as well as locality-specific employment law.	Agree	Add to pay plan policy.	Ralf Barnes/ Director	12/01/2024

*Entered in MM/DD/YYYY format. Generally, the date should be within 90 days (but no longer than 180 days) of report issuance. If the recommendation has already been implemented, enter the date it was implemented.