

# COUNTYWIDE JOURNAL ENTRY ASSURANCE ENGAGEMENT

Report No. AE-2024-6

---

AUGUST 6, 2024

---

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



# TABLE OF CONTENTS

AUDITOR’S LETTER.....1

FINDING(S) & OTHER MATTER(S) .....4

MANAGEMENT RESPONSE(S).....6

# AUDITOR'S LETTER



## Office of the County Auditor Internal Audit Division

August 6, 2024

Rodney Mann, Utah County Auditor  
Utah County Auditor's Office  
100 East Center Street, Suite 3600  
Provo, Utah 84606

Dear Mr. Mann:

The Internal Audit Division ("Division") performed an assurance engagement of Utah County Financial Information Systems ("COFIS") journal entries. During this limited review, we performed the following procedures:

1. For the period of October 1, 2023–December 31, 2023, tested a sample of COFIS General Ledger Module journal entries for valid and accurate documentation.
2. For the period of October 1, 2023–December 31, 2023, tested the population of COFIS General Ledger Module cancelled journal entries for valid documented cancellation reason.
3. For the period of October 1, 2023–December 31, 2023, tested a sample of COFIS General Ledger Module DEPT security user journal entries for the ability of each user to finalize any journal entry.
4. For the period of October 1, 2023–December 31, 2023, tested a sample of COFIS General Ledger Module DOALL security user journal entries for the ability of each user to finalize their own created journal entry.
5. For the period of October 1, 2023–December 31, 2023, tested the population of COFIS General Ledger Module REVIEW security users for the ability of each user to create a journal entry.
6. For the period of October 1, 2023–December 31, 2023, tested the population of COFIS General Ledger Module AUDITOR security users for the ability of each user to create a journal entry.

7. On and for July 29, 2024, tested the population of COFIS General Ledger Module users with DEPT, DOALL, and REVIEW security to determine if these security roles are assigned to Information Systems Department employee usernames.
8. On and for July 29, 2024, within a COFIS software testing environment, viewed an Information Systems Department employee independently verify that:
  - a. A user with DEPT security cannot finalize any journal entry.
  - b. A user with DOALL security cannot finalize their own created journal entry.
  - c. A user with REVIEW security cannot create a journal entry.
  - d. A user with AUDITOR security cannot create a journal entry.
  - e. A user who creates a journal entry, which is finalized by a separate user, cannot delete the finalized journal entry that they initially created.
  - f. A journal entry that has been finalized cannot be cancelled (i.e., deleted) following a month-end close.
  - g. Deleted journal entries (i.e., cancelled finalized journal entries) are saved in a log.
  - h. A user cannot edit a finalized or deleted journal entry.
  - i. A cancellation reason must be entered before a journal entry is cancelled.
  - j. A duplicated journal entry created from a previously finalized journal entry does not include original finalized journal entry dates.

The Division discovered one finding and two other matters during the engagement. For both finding(s) and other matter(s), we provide recommendations to improve the countywide accounting 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. We are pleased to note the Accounting Division collaborated with the Information Systems Department to successfully implement corrective action plans addressing two other matters reported in May 2023. Specifically, (1) a cancellation reason must be entered before a journal entry is cancelled and (2) a duplicated journal entry created from a previously finalized journal entry does not include original finalized journal entry dates.

The Division appreciates the courtesy and assistance extended to us by Accounting Division personnel during the engagement process and Information Systems Department personnel near the end of the engagement process. We look forward to a continuing professional relationship.

Sincerely,

Utah County Internal Audit Division

Utah County Auditor Internal Audit Division

CC: Danene Jackson, Associate Director of Financial Services, Utah County Auditor's Office  
Patrick Wawro, Director, Utah County Information Systems Department  
James Longhurst, Associate Director, Utah County Information Systems Department  
Jeff Wilkinson, Programming Division Manager, Utah County Information Systems Department

## FINDING(S) & OTHER MATTER(S)

### Finding 7.1: Insufficient Accounting and Programming Separation of Duties

#### Condition

We noted six Information Systems Department employees have COFIS usernames assigned DOALL security in the COFIS production environment.

#### 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 Organizations* (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."

Accounting is a business function and programming is a support function. In effect, programmers should have access only to development environments. Programmers should not have the ability to modify live data or access a production environment where data is stored and processed.

#### Cause

Information Systems Department management communicated the following reasons for employees retaining COFIS DOALL security:

1. Was a previous full-time employee that worked on COFIS in a greater capacity; later became a part-time, time-limited employee and was assigned to other responsibilities.
2. Project manager over COFIS team; may have participated in previous COFIS testing.
3. Unknown; may have completed temporary work for the COFIS team.
4. Unknown.
5. Active COFIS programmer; adds general ledger lines in the production environment to ensure Greenbelt program compliance until a feature-set with this functionality is rolled out to COFIS.
6. Active COFIS programmer.

Because the Information Systems Department does not currently have consistently enforced procedures regarding assigning and unassigning COFIS security access to Information Systems

Department employees, DOALL security access has remained for employees not actively working on COFIS and for employees actively working on COFIS.

**Effect**

COFIS General Ledger Module data integrity assurance is decreased due to:

- Increased likelihood of accidents, errors, financial misstatement, and concealment of financial misstatement; and
- Decreased likelihood of error and misstatement detection.

**Recommendation**

We recommend management remove DOALL security from being assigned to these six Information Systems Department employee COFIS usernames in the COFIS production environment.

**Other Matter 2.1: Duplicate Journal Entry Line Numbers**

**Condition**

We noted within the same journal entry with multiple line numbers, two different line numbers (which each had unique journal entry data) had duplicate line numbers (which each had unique journal entry data). The lack of unique line numbers did not appear to affect the arithmetic applied to the journal entry.

**Recommendation**

We recommend management configure COFIS to prevent duplicate line numbers from being created.

**Other Matter 3.1: Outdated DEPT Security Access**

**Condition**

We noted one COFIS username assigned DEPT security is associated with a former Utah County employee.

**Recommendation**

We recommend management remove DEPT security from this COFIS username and deactivate this COFIS username.

# MANAGEMENT RESPONSE(S)

## Finding 7.1: Insufficient Accounting and Programming Separation of Duties

### Management Response

Auditor’s note: This response was provided by Information Systems Department management.

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management remove DOALL security from being assigned to these six Information Systems Department employee COFIS usernames in the COFIS production environment.	Agree	We have removed DOALL access from the following employees: Ranjith Lakshman, Mike Johnson, Leena Kumar, and Brandon Davis. Mike Kniephof and Matt Bailey currently retain DOALL access to manage ongoing programming support duties. To ensure the integrity of the COFIS General Ledger, we will implement controls to properly manage COFIS security access for users and will also look at how we can efficiently and effectively utilize Separation of Duties (SoD) to manage business and support functions.	James Longhurst Associate Director – Information Systems	11/23/2024

\*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 2.1: Duplicate Journal Entry Line Numbers

### Management Response

Auditor’s note: This response was provided by Information Systems Department management.

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
We recommend management configure COFIS to prevent duplicate line numbers from being created.	Disagree	We have troubleshooted this issue in the past without success. We can look at this issue again if it is decided that a resolution is worth the resources needed to resolve. We are open to further discussion with affected parties to make that determination.	Mike Kniephof – Programming Team Supervisor	N/A

\*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 3.1: Outdated DEPT Security Access

### Management Response

Auditor’s note: This response was provided by Accounting Division management.

Recommendation	Agree/Disagree	Corrective Action Plan	Name and Title of Employee Responsible for Implementation	Target Date*
<p>We recommend management remove DEPT security from this COFIS username and deactivate this COFIS username.</p>	<p>Agree. This was a simple timing issue.</p> <p>When an employee separates from the County, the network username of that employee is deactivated by the IT department. COFIS security is based on that network username, meaning even if the COFIS security table shows the username, the user cannot transact in the system because no one can log on as that user even if someone else had the user’s password under circumstances not compliant with County IT policies. In addition, financial transactions require a secondary type of authorization to post to the general ledger.</p> <p>When employees separate from County employment, there is currently no communication process from either the HR Department or the IT Department to the Auditor’s Office that the employee has left County employment. Departments can notify the Auditor’s Office of a separating employee via a security change request form available on the Finance Hub. Most departments wait to do this until another employee is hired to the role so that security can be copied from the previous employee to the new employee.</p>	<p>The COFIS username identified was a separated employee. A new employee was hired to replace that employee effective August 5, 2024. On August 5, 2024, the department submitted a security change request form via the Finance Hub to copy the security from the previous employee to the new employee. This request was completed at approximately 3:15PM on August 5 and the previous employee’s username was deactivated at that same time. This letter is dated August 6, so the security for that COFIS username had been removed prior to the issuance of this report.</p> <p>Accordingly, no corrective action plan is needed.</p>	<p>Not Applicable</p>	<p>Not Applicable (08/05/2024)</p>

\*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.