SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

ITEM: 2.14
(ID # 20722)
MEETING DATE:
Tuesday, December 13, 2022

FROM : AUDITOR CONTROLLER:

SUBJECT: AUDITOR-CONTROLLER: Internal Audit Report 2023-005: Riverside County Flood Control & Water Conservation District Audit

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2023-005: Riverside County Flood Control & Water Conservation District Audit

ACTION:Consent

Tanya Harris

Tanya Harris, Assistant Auditor Controller 12/1/2022

MINUTES OF THE BOARD OF SUPERVISORS

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$ 0.0	$ 0.0	$ 0.0	$ 0.0
NET COUNTY COST	$ 0.0	$ 0.0	$ 0.0	$ 0.0
SOURCE OF FUNDS: N/A			**Budget Adjustment: No**	
			For Fiscal Year: n/a	

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

Summary

In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Flood Control & Water Conservation District. This audit is conducted to provide management and the Board of Supervisors with an independent assessment of internal controls over system access controls.

Based upon the results of our audit, we identified opportunities for improvement of internal controls relating to system access controls.

We will follow-up in one year to determine if actions were taken to correct the findings noted.

Impact on Citizens and Businesses

Provide an assessment of internal controls over the audited areas.

SUPPLEMENTAL:

Additional Fiscal Information

Not applicable

ATTACHMENTS:

A: Riverside County Auditor-Controller's Office - Internal Audit Report 2023-005: Riverside County Flood Control & Water Conservation District Audit

Internal Audit Report 2023-005

Riverside County Flood Control & Water Conservation District Audit

Report Date: December 13, 2022

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Office of Paul Angulo, CPA, MA
Riverside County Auditor-Controller
4080 Lemon Street, 11th Floor
Riverside, CA 92509
(951) 955-3800

www.auditorcontroller.org

COUNTY OF RIVERSIDE
OFFICE OF THE
AUDITOR-CONTROLLER

County Administrative Center
4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
(951) 955-3800
Fax (951) 955-3802

Paul Angulo, CPA, M.A.
Riverside County Auditor-Controller

Tanya S. Harris, DPA, CPA
Assistant Auditor-Controller

December 13, 2022

Jason Uhley
General Manager – Chief Engineer
Riverside County Flood Control & Water Conservation District
1995 Market St.
Riverside, CA 92501

Subject: **Internal Audit Report 2023-005: Riverside County Flood Control & Water Conservation District Audit**

Dear Mr. Uhley:

In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Flood Control & Water Conservation District to provide management and the Board of Supervisors with an independent assessment of internal controls over system access controls.

We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain sufficient, reliable, relevant and useful information to provide reasonable assurance that our objective as described above is achieved. An internal audit includes the systematic analysis of information to evaluate and improve the effectiveness of internal controls. We believe this audit provides a reasonable basis for our conclusion.

Internal controls are processes designed to provide management reasonable assurance of achieving efficiency of operations, compliance with laws and regulations, and reliability of financial and non-financial information. Management is responsible for establishing and maintaining adequate internal controls. Our responsibility is to evaluate the internal controls.

Our conclusion and details of our audit are documented in the body of this audit report.

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Internal Audit Report 2023-005: Riverside County Flood Control & Water Conservation District Audit

As requested, in accordance with paragraph III.C of the Board of Supervisors Resolution 83-338, management responded to each reported condition and recommendation contained in our report. Management's responses are included in the report. We will follow-up to verify that management implemented the corrective actions.

Paul Angulo, CPA, MA
Riverside County Auditor-Controller

By: René Casillas, CPA, CRMA
Deputy Auditor-Controller

cc: Board of Supervisors
Jeff A. Van Wagenen, Jr., County Executive Officer
Dave Rogers, Chief Administrative Officer
Grand Jury

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Internal Audit Report 2023-005: Riverside County Flood Control & Water Conservation District Audit

Table of Contents

Page

Executive Summary 4

Results:

System Access Controls 6

Internal Audit Report 2023-005: Riverside County Flood Control & Water Conservation District Audit

Executive Summary

Overview

Riverside County Flood Control & Water Conservation District (Flood Control) was created in 1945 following the floods of 1938. Flood Control oversees 2,700 square miles of stormwater management of the western part of the county. It is also responsible for planning, designing, constructing, and operating regional storm drains, channels, levees, and dams.

Flood Control has an adopted budget of $212.9 million for FY 2022-23 and 320 adopted positions. *County of Riverside, Fiscal Year 2022-23 Adopted Budget Volume 1, 298-299.*

Audit Objective

Our objective is to provide management and the Board of Supervisors with an independent assessment about the adequacy and effectiveness of internal controls over system access controls. Internal controls are processes designed to provide management reasonable assurance of achieving efficiency of operations, compliance with laws and regulations, and reliability of financial and non-financial information. Reasonable assurance recognizes internal controls have inherent limitations, including cost, mistakes, and intentional efforts to bypass internal controls.

Audit Scope and Methodology

We conducted the audit from June 1, 2022, through August 29, 2022, for operations from June 1, 2021, through August 24, 2022. Following a risk-based approach, our scope initially included the following:

- Construction Contracts
- Disaster Mitigation and Recovery Plan
- Maintenance Service Agreements
- System Access Controls

Through inquiry, observations, and limited examination of relevant documentation, it was determined through a risk assessment of construction contracts, disaster mitigation and recovery plan, and maintenance service agreements, that the risk exposure to Flood Control associated with these processes are well mitigated with internal controls and

are functioning as designed. Therefore, our audit scope focused on internal controls over system access controls.

Audit Highlights

Summary of Existing Conditions

- Terminated employees did not have their Active Directory account termination requests created and approved in a timely manner (within 24 hours). Allowing active directory accounts to remain open after employment has ended exposes the department to risk where information maintained in department systems can be continuously accessed by individuals who no longer have a right or need to know. Depending on the sensitivity of the information maintained by department systems, it can create administrative issues and have a financial impact if held liable.

Summary of Improvement Opportunities

- Ensure compliance with County of Riverside Information Security Standard v1.0, Section 4.1, *Account and Access Management*, by disabling Active Directory accounts on the day of an employee's termination or transfer from the department.

- Develop policies and procedures to ensure the disabling of Active Directory accounts are requested and approved within 24 hours of an employee's termination or transfer from the department.

Audit Conclusion

Based upon the results of our audit, we identified opportunities for improvement of internal controls relating to system access controls.

System Access Controls

Background

System access controls within information systems ensure proper confidentiality, integrity, and availability to the data stored within the system. Authentication is a control which confirms a user's identity to provide access to a systems sensitive information. Sensitive information is any information that must be protected from unauthorized access to maintain the information security of an organization or an individual. Authentication is often achieved by using login credentials such as a username and password. Authentication relies on the presumption that the user is authorized to use the system and that only the user knows the login credentials to gain access.

Active Directory is a directory service which allows Flood Control to manage permissions and access to network resources, and linked data applications utilized by the department. When a user ends employment with Flood Control, it is the department's responsibility to create and approve a help desk ticket to request the removal of the terminated employee's access rights to their Active Directory account. Once the ticket is approved by Flood Control personnel, Riverside County Information Technology (Information Technology) is notified to disable Active Directory to remove permissions and network access. These help desk tickets contain various workflow tasks such as disabling e-mail accounts, active directory, data/application systems access, badge access, reclaiming software licenses, and reclaiming any equipment that may have been issued to an employee. A help desk ticket is not closed until all tasks within have been completed by Information Technology personnel.

Objective

To verify the existence and adequacy of internal controls over employee access termination to system applications used by Flood Control.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of County of Riverside Information Security Standard v1.0.

- Interviewed key personnel regarding the department's employee access termination processes.

- Obtained a listing of all critical systems used by Flood Control and judgmentally selected a sample of systems not linked to Active Directory.

- Obtained listing of employees who had access to the selected system applications not linked to Active Directory during the audit review period.

- Obtained listing of employees whose access to the selected system applications not linked to Active Directory were terminated during the audit review period.

- Obtained report from Information Technology that details Flood Control ticket creation and approval dates for disabling employee access to Active Directory.

- Verify access rights to the selected system applications not linked to Active Directory were disabled within 24 hours of an employee's termination from Flood Control.

- Verify whether requests to disable Active Directory were created and approved by Flood Control personnel within 24 hours of an employee's termination or transfer from the department.

Finding 1: Timely Termination of Access Rights

Upon termination or transfer from Flood Control, 22 out of a total of 36 employees (61%) did not have their Active Directory account termination requests created and approved in a timely manner (within 24 hours). Of the 22 untimely account termination requests, 2 Active Directory accounts remained active as a request was not initiated to terminate the accounts. For the remaining 20 employees whose Active Directory accounts were disabled, the average time elapsed between employee termination and ticket approval was 14 days, with the longest taking 69 days for approval and the shortest taking 4 days. County of Riverside Information Security Standard v1.0, Section 4.1, *Account and Access Management*, states, "Accounts for terminated or transferred employees shall be disabled or removed on the day of termination or transfer." Requests and approvals to disable Active Directory accounts are not created and approved in a timely manner after employees are terminated or transferred from the department. Flood Control's current policies and procedures do not include a process to

ensure user accounts for terminated or transferred employees are to be disabled or removed on the day of termination or transfer. Allowing active directory accounts to remain open after employment has ended exposes the department to risk where information maintained in department systems can be continuously accessed by individuals who no longer have a right or need to know. Depending on the sensitivity of the information maintained by department systems, it can create administrative issues and have a financial impact if held liable.

Recommendation 1.1

Ensure compliance with County of Riverside Information Security Standard v1.0, Section 4.1, *Account and Access Management*, by disabling Active Directory accounts on the day of an employee's termination or transfer from the department.

Management's Response

"**Concur**. The District should ensure compliance with County policy by requesting the termination of Active Directory accounts within 24 hours of an employee's separation from the District."

Actual/Estimated Date of Corrective Action: October 6, 2022

Recommendation 1.2

Develop policies and procedures to ensure the disabling of Active Directory accounts are requested and approved within 24 hours of an employee's termination or transfer from the department.

Management's Response

"**Concur**. On October 6, 2022, the District implemented Policy B-24, *Procedure for Removing Computer and Application Access*, documenting the requirement to request and approve disabling Active Directory accounts within 24 hours of an employee's separation from the District. The District also provided supervisors and managers an updated termination checklist outlining the requirements for disabling Active Directory and non-Active Directory user accounts."

Actual/Estimated Date of Corrective Action: October 6, 2022