PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

First Follow-Up Information Technology Audit: OC Waste & Recycling Selected Cybersecurity Controls As of March 31, 2026

Audit No. 2413-F1
Report Date: September 10, 2026

Recommendation Status

3	Implemented
1	In Process
0	Not Implemented
0	Closed

OC Board of Supervisors

CHAIR DOUG CHAFFEE	VICE CHAIR KATRINA FOLEY	SUPERVISOR JANET NGUYEN	SUPERVISOR VICENTE SARMIENTO	SUPERVISOR DONALD P. WAGNER
4th DISTRICT	5th DISTRICT	1st DISTRICT	2nd DISTRICT	3rd DISTRICT

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 2413-F1

September 10, 2026

To: Tom Koutroulis
OC Waste & Recycling Director

From: Aggie Alonso, CPA, CIA, CRMA
Internal Audit Department Director

Digitally signed by Aggie Alonso
Date: 2026.09.10 15:45:34 -07'00'

Subject: First Follow-Up Information Technology Audit: OC Waste & Recycling Selected Cybersecurity Controls

---

We have completed a follow-up audit of OC Waste & Recycling (OCWR) Selected Cybersecurity Controls administered or monitored by OCWR, original Audit No. 2413 dated September 3, 2025. Due to the sensitive nature of specific findings (restricted information), certain results are redacted from public release Additional information, including background and our scope, is included in Appendix A.

We followed up on the status of the four recommendations from our original audit and concluded that OCWR implemented three recommendations and is in process of implementing the remaining recommendation. A second follow-up audit will be performed in approximately six months, and we will provide a follow-up form to facilitate that audit. Any recommendations still in process at that time will be brought to the attention of the Audit Oversight Committee at its next scheduled meeting.

We appreciate the assistance extended to us by OCWR personnel during our follow-up audit. If you have any questions, please contact me at (714) 834-5442 or Deputy Director Jose Olivo at (714) 834-5509.

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
County Executive Office Distribution
OCWR Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board
Crowe LLP, County External Auditor

INTERNAL AUDIT DEPARTMENT

RESULTS

FINDING NO. 1	**Password Configuration Settings** OCWR's [redacted] password settings did not conform to the minimum length, complexity, history, or expiration requirements set by the County's Cybersecurity Policy, Section 9.2.7 Passwords.
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	OCWR management collaborate with the [redacted] system vendor to strengthen password settings to include minimum length, complexity, history, and expiration; where technically feasible, to properly manage passwords; and protect against unauthorized discovery or usage, in accordance with County Cybersecurity policy requirements.
STATUS	**Implemented.** We noted that OCWR collaborated with the [redacted] system vendor to strengthen password settings to include the recommended configurations. We reviewed the modified password configurations and confirmed that the current settings conform to the County's Cybersecurity Password Policy. Based on the actions taken, we consider this recommendation implemented.

FINDING NO. 2	Content has been removed due to sensitive nature of the specific findings.
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	Content has been removed due to sensitive nature of the specific findings.
STATUS	**In Process.** Content has been removed due to sensitive nature of the specific findings.

FINDING NO. 3	**User Account Creation Process** OCWR did not have a formalized process for creating new user accounts in the [redacted] system. New user accounts were requested through various informal methods including email, an access request form, or a help desk ticket, which were not consistently retained as required by the County's Cybersecurity Policy, Section 8.2.5 Access Controls.
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	OCWR management formalize their process to ensure new user account requests are consistently approved and documented prior to provisioning user accounts in [redacted], so that only users with legitimate business needs are granted access.

STATUS	**Implemented.** We noted that OCWR formalized a process for creating new user accounts in the [redacted] system by establishing a written procedure and an access request form. For all new user account access requests, the supervisor is now required to complete and submit an online User Provisioning form to request access. The form is then reviewed by OCWR IT staff, who are responsible for verifying legitimate business need prior to provisioning access. We reviewed the referenced online form and confirmed that it included the necessary [redacted] system access request details and that required approvals are documented. Based on the actions taken, we consider this recommendation implemented.

FINDING NO. 4	**Department IT Procedures** OCWR did not have IT procedures for Identity and Access Management and Vulnerability Management. Although they have documented procedures regarding security implementation and deployment of computing hardware, software, mobile, cloud services, and storage devices, we noted that the procedures have not been updated since July 2016.
CATEGORY	**Control Finding**
RECOMMENDATION	OCWR management: A. Establish documented procedures for Identity and Access Management and Vulnerability Management. B. Establish a process to periodically review and update departmental procedures to ensure they are accurate and contain relevant information.
STATUS	**Implemented.** We noted that OCWR established documented procedures for Identity and Access Management and Vulnerability Management. We reviewed the procedures document titled "Access and Account Management Controls" over [redacted] and confirmed: • **Identity and Access Management** – OCWR established and strengthened its processes for granting, reviewing, and documenting user access and deprovisioning to the [redacted] application to ensure that the appropriate level of access is granted to perform job duties, limit access to those with direct business need, and deactivate users in a timely manner. For example, OCWR requires the completion of a User Provisioning Form and submission of an IT helpdesk ticket to document the request for provisioning and deprovisioning until the task is completed. • **Vulnerability Management** – OCWR is now part of OC Information Technology Shared Services who leverages the existing County

	Vulnerability Management Policy, which states that vulnerability scans be performed at a frequency sufficient to detect and mitigate vulnerabilities within the time frames designated by the County Patch Management Policy, with scans conducted at least monthly. In addition, we noted that OCWR established a written policy requiring an annual review of departmental procedures to ensure continued accuracy and relevance. OCWR is scheduled to perform next review in January 2027. Based on the actions taken, we consider this recommendation implemented.

AUDIT TEAM	Jimmy Nguyen, CISA, CFE, CEH	Senior IT Audit Manager
	JC Lim, CIA, CISA, CFE	Administrative Services Manager

INTERNAL AUDIT DEPARTMENT

APPENDIX A: ADDITIONAL INFORMATION

SCOPE	Our follow-up audit was limited to reviewing actions taken by OCWR as of March 31, 2026, to implement the four recommendations from our original audit dated September 3, 2025.
BACKGROUND	In the original audit, we reviewed selected cybersecurity controls administered or monitored by OCWR and identified three Significant Control Weaknesses and one Control Finding.

APPENDIX B: FOLLOW-UP AUDIT IMPLEMENTATION STATUS

Implemented	In Process	Not Implemented	Closed
The department has implemented our recommendation in all respects as verified by the follow-up audit. No further follow-up is required.	The department is in the process of implementing our recommendation. Additional follow-up may be required.	The department has taken no action to implement our recommendation. Additional follow-up may be required.	Circumstances have changed surrounding our original finding/ recommendation that: (1) make it no longer applicable or (2) the department has implemented and will only implement a portion of our recommendation. No further follow-up is required.