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

ITEM: 2.6
(ID # 30276)
MEETING DATE:
Tuesday, April 28, 2026

FROM : AUDITOR CONTROLLER

SUBJECT: AUDITOR-CONTROLLER: Internal Audit Report 2026-005 Riverside County Information Technology Audit, [District All); [$0]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2026-005: Riverside County Information Technology Department Audit

ACTION:Consent

Ben J. Benoit, COUNTY AUDITOR-CONTROLLER 4/16/2026

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Washington, seconded by Supervisor Perez and duly carried by unanimous vote, IT WAS ORDERED that the above matter is received and filed as recommended.

Ayes:	Medina, Spiegel, Washington, Perez, and Gutierrez
Nays:	None
Absent:	None
Date:	April 28, 2026
xc:	Auditor

Kimberly A. Rector
Clerk of the Board
By: _____
Deputy

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

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 Information Technology Department to provide management and the Board of Supervisors with an independent assessment of internal controls over legacy systems management, non-capital asset management, artificial intelligence governance, and procurement card management.

Based on the results of our audit, we determined that internal controls over AI governance and procurement card are functioning as designed to help Information Technology achieve its business process objectives. However, we have identified improvement opportunities for internal controls over legacy system management and non-capital assets that can help provide reasonable assurance that the department's objectives over these areas will be achieved. Specifically, improvements are needed to ensure legacy end of life system management procedures are established, and non-capital assets were tracked, updated, and inventoried on periodic basis.

Impact on Citizens and Businesses

Provide an assessment of internal controls over the audited areas.

SUPPLEMENTAL:

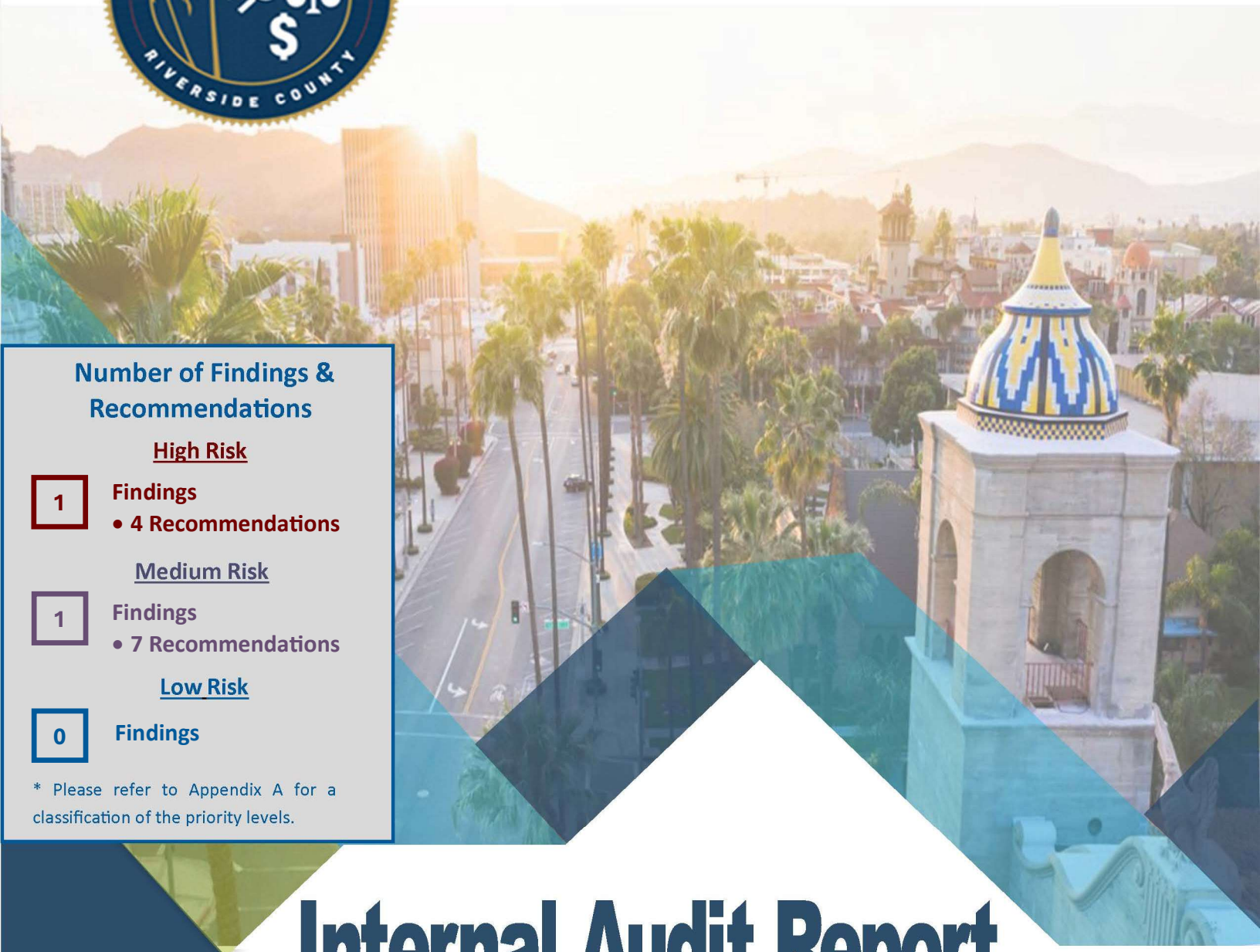
Additional Fiscal Information

Not applicable

ATTACHMENTS:

A: Riverside County Auditor-Controller's Office - Internal Audit Report 2026-005: Riverside County Information Technology Department Audit.

Office of Ben J. Benoit
Riverside County Auditor-Controller



Number of Findings & Recommendations

High Risk

1 Findings
- 4 Recommendations

Medium Risk

1 Findings
- 7 Recommendations

Low Risk

0 Findings

* Please refer to Appendix A for a classification of the priority levels.

Internal Audit Report

2026-005

Riverside County
Information Technology Department

April 28, 2026

COUNTY OF RIVERSIDE
OFFICE OF THE AUDITOR-CONTROLLER
BEN J. BENOIT
AUDITOR-CONTROLLER
TANYA S. HARRIS, DPA, CPA | JON JENSEN, CPP
ASSISTANT AUDITOR-CONTROLLER

April 28, 2026

Karan Chandran
Chief Information Officer
Riverside County Information Technology Department
3450 Fourteenth Street
Riverside, CA 92501

Subject: **Internal Audit Report 2026-005: Riverside County Information Technology Department Audit**

Dear Mr. Chandran:

In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Information Technology Department to provide management and the Board of Supervisors with an independent assessment of internal controls over legacy systems management, non-capital asset management, artificial intelligence governance, and procurement card management.

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 a 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 internal controls.

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

Internal Audit Report 2026-005: Riverside County Information Technology Department 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.

We thank you and your staff for the help and cooperation. The assistance provided contributed significantly to the successful completion of this audit.

Ben J. Benoit
Riverside County Auditor-Controller

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

cc: Board of Supervisors
Jeff A. Van Wagenen, Jr., County Executive Officer
Juan Perez, Chief Operating Officer
Don Kent, Chief Finance Officer
Sarah Franco, Assistant Chief Executive Officer
Grand Jury

Table of Contents

Page

Executive Summary.....4

Results:

Legacy System Management 6

Non-Capital Asset Management 9

Artificial Intelligence Governance.....16

Procurement Card Management.....17

Appendix A: Finding Priority Level Classification.....21

Executive Summary

Overview

Riverside County Information Technology (Information Technology) is responsible for planning, designing, implementing, operating, and coordinating the county's information and communications technology. The department's services include the following: Countywide Cyber Security, Geographic Information Services (GIS), RivCoTV, Network, Wireless, Managed Technology Services, and Digital Equity Program. Information Technology manages 27 separate county departments.

Information Technology has an adopted budget of $122.5 million for FY 2025-26 and 396 adopted positions. *County of Riverside, Fiscal Year 2025-26 Adopted Budget Volume 1, 206-207.*

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 legacy systems management, non-capital asset management, artificial intelligence governance, and procurement card management. 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 HIGHLIGHTS

- Improvements are needed to ensure legacy systems are identified, tracked, reviewed, and managed.
- Processes for tracking, updating, and periodically inventorying non-capital assets can be improved.

Audit Scope and Methodology

We conducted the audit from September 9, 2025, through January 31, 2026, for operations from July 1, 2023, through January 16, 2026. Using a risk-based approach, our scope included the following:

- Legacy Systems Management
- Non-Capital Asset Management
- Artificial Intelligence Governance
- Procurement Card Management

Audit Conclusion

Based on the results of our audit, we determined that internal controls over AI governance and procurement card are functioning as designed to help Information Technology achieve its business process objectives. However, we have identified improvement opportunities for internal controls over legacy system management and non-capital assets that can help provide reasonable assurance that the department's objectives over these areas will be achieved. Specifically, improvements are needed to ensure legacy end of life system management procedures are established, and non-capital assets were tracked, updated, and inventoried on periodic basis.

Legacy Systems Management

Background

Information Technology manages a portfolio of County system servers hosting multiple applications and web servers that continue to support critical County operations. These systems include hardware, software, and applications that regularly receive vendor support and security updates to mitigate operational or security risk. Information Technology oversees the respective systems to maintain continuity of services while assessing modernization, replacement, or retirement options.

Information Technology is responsible for establishing oversight and management practices to ensure systems remain functional, secure, and compliant with applicable County policies and regulatory requirements. This includes evaluating system risk, monitoring system performance, and coordinating with departments to determine appropriate mitigation strategies. Such strategies may include compensating controls or planned system replacements.

Systems and applications that are discontinued no longer receive security updates and are classified as end-of-life legacy systems. The absence of security updates increases vulnerability to cyber threat actors and requires proper identification, tracking, and communication.

Legacy systems management consists of defined governance practices, controls assessment processes, and ongoing monitoring activities designed to address operational, security, and compliance risks associated with aging technology.

Objective

To verify the existence and adequacy of internal controls over legacy systems management.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of board policies A-55 Electronic Government Policy (E-Government), and applicable Information Security Standard 2.0, National Institute of Standards and Technology publication 800-53, Center of Internet Security, *Critical Security Controls V8*, over Legacy system management.

- Requested and obtained reports used to track costs associated with maintaining legacy systems including licensing, vendor contracts, and internal labor.

- Evaluated whether management conducts periodic reviews to reassess system risk and operational viability.
- Evaluated how incidents are logged and reviewed to prevent data loss or extended disruptions.
- Assessed how unresolved vulnerabilities are tracked and communicated to management and whether corrective actions are documented or monitored for completion.
- Determined how the department enforce controls to secure legacy systems.

Finding 1: Legacy System Management	Priority Level 1[1]

Information Technology Standard, *Unsupported System Component*, states, "IT Administrators shall replace system components when support for the components is no longer available from the developer, vendor, or manufacturer." Additionally, National Institute of Standards and Technology's NIST SP 800-53, *System Development Lifecycle Control Enhancement (3*), "The use of obsolete or nearing obsolete technology may increase the security and privacy risks associated with unsupported components." Lastly, Center of Information Security, *Inventory and Control of Software*, *Safeguards 2.2*, states, "Only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance."

A review of all County's applications and system servers managed by Information Technology identified 130 legacy systems that had exceeded end-of-life status. These systems were not formally identified, tracked, or managed through a defined lifecycle management approach. Information Technology procedures to support documentation, communication, and planning for system upgrades or extended vendor security agreement were not established. As a result, centralized visibility into legacy system risks is limited, which affects the County's ability to proactively manage system obsolescence and related operational and security considerations.

Recommendation 1.1

Establish system end-of-life management procedures that define roles, responsibilities, and expectations for identifying, tracking, reviewing, and managing legacy systems.

[1] Please see Appendix A (page 21) for a description of the finding priority level classifications.

Management's Response

"**Concur**. RCIT will review and enhance our existing end-of-life management procedures to ensure they clearly document the specific roles, responsibilities, and expectations required for the consistent identification, tracking, review, and management of legacy systems. This effort will include defining standardized criteria for determining end-of-life status, establishing documented workflows for system evaluation, and outlining the communication and approval processes needed when legacy systems are retained. These procedures will also delineate responsibilities for both RCIT and the supported departments to promote coordinated decision-making, ensure accountability throughout the system lifecycle, and strengthen the County's overall governance and risk-management posture."

Actual/estimated Date of Corrective Action: August 1, 2026

Recommendation 1.2

Develop and maintain a centralized inventory of application and system servers, including identification of systems that have exceeded end-of-life status.

Management's Response

"**Concur**. RCIT currently utilizes a centralized tool to maintain our server inventory. While this system effectively tracks core server information, it does not currently include fields for extended support status. We can, however, evaluate options for establishing a centralized location to capture and maintain this additional data. RCIT has recently purchased additional ServiceNow modules that may assist with tracking application and server information in a common CMDB. RCIT will establish procedures to track and maintain inventory of these items."

Actual/estimated Date of Corrective Action: August 1, 2026

Recommendation 1.3

Establish extended security update agreements, as applicable, to maintain security coverage during transition periods when system upgrades cannot be completed immediately.

Management's Response

"**Concur**. To support extended security update agreements, when servers are running department-specific software, the associated costs for these updates must be treated as pass-through expenses. Department approval is required before incurring these costs. If third-party

applications are involved, compatibility must be verified with the vendor. Extended service agreements depend on departmental acceptance of charges and vendor approval, but RCIT will keep communicating and tracking any risks if mitigation is not achieved. Records will be maintained to monitor the status of extended security agreements and any mitigating controls."

Actual/estimated Date of Corrective Action: August 1, 2026

Recommendation 1.4

Ensure applicable NIST and CIS recommended controls for legacy system management are incorporated into control assessment checklists when legacy systems are carried forward.

Management's Response

"**Concur**. RCIT will review our existing assessment checklists and partner with ISO (Information Security Office) to identify any gaps and incorporate the applicable NIST and CIS recommended controls for legacy system management for systems retained going forward."

Actual/estimated Date of Corrective Action: August 1, 2026

Non-Capital Asset Management

Background

Non-capital assets, also known as "walk-away" assets, are tangible items that do not meet county capitalization thresholds, generally defined as assets with an acquisition cost of less than $10,000, but still require safeguarding due to their portability, value, or sensitivity. These assets may include, but are not limited to, laptop computers, tablets, cellular phones, network transceivers, power distribution switches, and rack servers– all of which are vulnerable to loss, theft, or misuse if not properly tracked. While not recorded in the capital asset ledger, non-capital assets are often maintained through departmental tracking systems or inventories. Effective management of non-capital assets involves identifying items subject to tracking, labeling or tagging where appropriate, maintaining accurate records of location and custody, and conducting periodic physical inventories to confirm existence and condition. Adequate internal controls in this area help ensure accountability and promote responsible stewardship of public property.

Information Technology's asset management system maintains asset records for non-capital equipment and has the capability to track inventory and assignment information. This includes service status designations reflected in the "state" field, such as "in stock," in use," in transit," or retired." The system also retains activity history associated with asset records. Maintaining accurate status information supports inventory tracking, accountability, and monitoring of asset availability across facilities.

Objective

To verify the existence and adequacy of internal controls over Information Technology's non-capital asset management.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of Board Policy Number H-26, *Non-Capitalized Asset Management*, and applicable standards over non-capital asset management.
- Conducted interviews with key personnel to gain an understanding of the department's non-capital asset management process.
- Verified whether there was adequate segregation of duties in place relating to non-capital asset management processes.

- Obtained a listing of all non-capital assets internally tracked by the department.
- Selected a random sample of non-capital assets and verified physical existence, location, asset tag, serial number, and operational condition.
- Identified additional non-capital assets during fieldwork and verified whether they were included in the department's internal asset tracking listing.
- Assessed the adequacy of physical security controls in areas where non-capital assets were stored or used.
- Obtained a listing of non-capital assets disposed of during the audit review period and selected a sample for review.
- Verified whether asset disposals were properly documented and processed in accordance with Board Policy H-26 and internal policies.
- Obtained a listing of non-capital assets disposed of during the audit review period and selected a sample for review.
- Verified whether lost assets incidents were reported to the appropriate authorities and investigated in accordance with applicable policy requirements.
- Obtained a listing of active and separated employees during the audit review period and selected a sample for review to verify whether assets were still assigned to separated employees.

Finding 2: Non-Capital Asset Management	Priority Level 2[2]

County of Riverside Board of Supervisor's Policy H-26, Non-Capitalized Asset Management, states, "Non-capitalized assets which are small, mobile, easily converted to personal use, and have a fair market value of at least $200 are classified as 'walk-away assets...' Each department shall ensure compliance with this policy by tracking walk-away assets using the county's Asset Management Module… Departments may use another established system to ensure the accountability of non-fixed assets…" Additionally, Government Finance Officers Association recommends that governments should ensure adequate internal controls are in place for items that are not capitalized but still require special attention due to legal compliance, public safety, or theft risk.

[2] Please see Appendix A (page 21) for a description of the finding priority level classifications.

Based on asset verification testing of 48 non-capital assets and a review of 14 non-capital assets designated as missing in the department's asset management system, the following conditions were identified.

Of the 48 sampled assets, 25 assets (52%) had one or more exceptions, as detailed below:

- Eighteen assets could not be physically located, and supporting documentation was not available to confirm existence.

- Three assets were maintained in a legacy spreadsheet and were not transferred into Information Technology's current asset management system during system implementation in 2018.

- Two assets were incorrectly classified as non-capital assets instead of supplies inventory items.

- One asset remained in "In Transit" status since September 2024, the respective asset was observed as "In Use."

- One asset was not located at the address recorded in the Information Technology asset management system.

Separately, of the 14 assets designated as missing assets, eight non-capital assets (57%) did not include supporting documentation or evidence of supervisory approval for the status change to "Missing."

In addition, a separated employee remained listed in the Information Technology asset management system as the assigned custodian for multiple non-capital assets, including a County-issued laptop. Asset records were not updated to reflect recovery, reassignment, or return-to-stock status.

These conditions occurred due to variations in asset routing, deployment, recovery, and inventory management practices. Additionally, the communication of the status of asset changes were not routinely maintained or updated in timely, and physical inventory counts were not conducted. Lastly, standardized procedures can be established to highlight correct asset classification, lost-assets documentation, and employee separation notifications.

Consequently, asset records did not consistently reflect up-to-date view of asset location, custody, and status. This limits the department's ability to reliably verify asset existence and maintain effective inventory oversight.

Recommendation 2.1

Develop, document, and implement periodic physical inventory verification and reconciliation procedures.

Management's Response

"**Concur**. We agree that formalized, documented physical inventory verification and reconciliation procedures will strengthen asset accountability and improve data accuracy within the Information Technology asset management system. While elements of this process currently occur, they are not consistently documented or standardized. We will establish and implement a recurring inventory schedule and develop written procedures to ensure uniform application across all teams."

Actual/estimated Date of Corrective Action: November 1, 2026

Recommendation 2.2

Standardize procedures for asset routing, deployment, and status updates to ensure asset movements and custody changes are consistently recorded into the Information Technology asset management system.

Management's Response

"**Concur**. We agree that standardized procedures are necessary for consistent recording of non-asset movements and custody changes. Current workflows vary by team, which can result in inconsistent data entry. We will develop and publish standardized routing and deployment procedures and ensure staff follow a uniform process for updating the non-asset management system."

Actual/estimated Date of Corrective Action: November 1, 2026

Recommendation 2.3

Implement periodic training for deployers and technicians on asset routing responsibilities, deployment procedures, and required status and location updates within the Information Technology asset management system.

Management's Response

"**Concur**. We agree that recurring training is essential to maintaining compliance with non-asset management requirements. Providing regular refresher training will help ensure deployers and technicians follow proper procedures and maintain accurate and timely system updates. Training materials and schedules will be developed and implemented."

Actual/estimated Date of Corrective Action: November 1, 2026

Recommendation 2.4

Implement management monitoring controls using existing Information Technology asset management system reports to periodically review high-risk asset status exceptions (such as assets remaining in "In Transit," inactive employee assignments, and unassigned assets) and ensure timely resolution of identified issues.

Management's Response

"**Concur**. We agree that management monitoring using available system reports will strengthen oversight and improve the timely resolution of non-asset status exceptions. Implementing a recurring review process will help identify and address non-assets that remain in high-risk categories. We will develop monitoring protocols and designate responsible reviewers."

Actual/estimated Date of Corrective Action: November 1, 2026

Recommendation 2.5

Develop and communicate formal asset classification and categorization guidance, including standardized use of asset identifiers within the Information Technology asset management system.

Management's Response

"**Concur**. We agree that formal guidance is needed to ensure non-assets are consistently classified, categorized, and identified within the system. Standardizing these elements will improve reporting accuracy and streamline non-asset lifecycle tracking. We will develop written guidance and communicate it to all stakeholders."

Actual/estimated Date of Corrective Action: November 1, 2026

Recommendation 2.6

Develop and implement formal policies and desk procedures governing the handling of missing or stolen non-capital assets, including required documentation, approval workflows, escalation protocols, and asset status update requirements within the Information Technology asset management system.

Management's Response

"**Concur**. We agree that formal policies and desk procedures are necessary to ensure missing or stolen non-capital assets are handled consistently, with appropriate documentation, approvals, and system updates. Establishing these procedures will enhance accountability and compliance with reporting requirements. We will ensure these elements are incorporated into the updated procedures."
Actual/estimated Date of Corrective Action: November 1, 2026

Recommendation 2.7

Revise the employee separation process to require verification of asset return and forwarding of completed checklists to the Information Technology asset management team, ensuring timely updates to asset records.

Management's Response

"**Concur**. We agree that revisions to the separation process are needed to ensure timely and accurate return of non-assets and proper updates to non-asset records. Integrating non-asset verification steps into the process and ensuring completed checklists are submitted to IT asset management will reduce risk and improve tracking accuracy. We will update the employee separation checklist to include an additional step of confirming the return of all non-assets by the departing employee. "

Actual/estimated Date of Corrective Action: November 1, 2026

Artificial Intelligence

Background

Riverside County Information Technology (Information Technology) has established a Generative Artificial Intelligence (GenAI) Use Policy to provide a secure, ethical, and controlled framework for the use of GenAI technologies. As part of this effort, Information Technology is exploring the use of GenAI across three primary areas: personal assistant GenAI tools, GenAI embedded within third-party applications, and custom applications developed through GenAI platforms. The policy applies to all Information Technology employees, contractors, temporary assignment personnel, and volunteers.

The Information Technology Department's Information Technology *GenAI Use Policy* authorizes the Chief Information Officer (CIO), or an authorized designee, to approve all GenAI systems, their acceptable uses, and authorized user groups prior to use, implementation, or development for any County department functions. This approval structure establishes centralized oversight and accountability for the use of GenAI technologies within the department.

The GenAI Use Policy consists of defined governance roles, approval processes, and usage standards that collectively establish oversight for GenAI technologies. The policy outlines requirements for evaluating, approving, and monitoring GenAI systems and defines controls related to authorization, training, data protection, transparency, and ongoing oversight to mitigate operational, legal, and information security risks. These requirements are maintained and updated as necessary by Information Technology to address evolving GenAI technologies and associated risks.

Objective

To verify the existence and adequacy of internal controls over Artificial Intelligence (AI) Governance.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of Board Policy *A-50 Electronic Media and Use Policy* and *Riverside County Information Technology GenAI Use Policy*.
- Interviewed key personnel and reviewed Information Technology department procedures over AI Governance.

- Obtained and reviewed training materials related to AI ethics, data privacy, or responsible AI use.

- Obtained and reviewed system documentation describing how sensitive data is protected within AI tools.

- Verified whether adequate safeguards are in place to prevent the use or storage of sensitive or personally identifiable information in IA models without proper authorization.

Finding: None Noted	Priority Level: N/A

Based on the results of our audit, we determined that internal controls over artificial intelligence governance provide reasonable assurance that its objective related to this area will be achieved. Reasonable assurance recognizes internal controls have inherent limitations, including cost, mistakes, and intentional efforts to bypass internal controls.

Procurement Card Management

Background

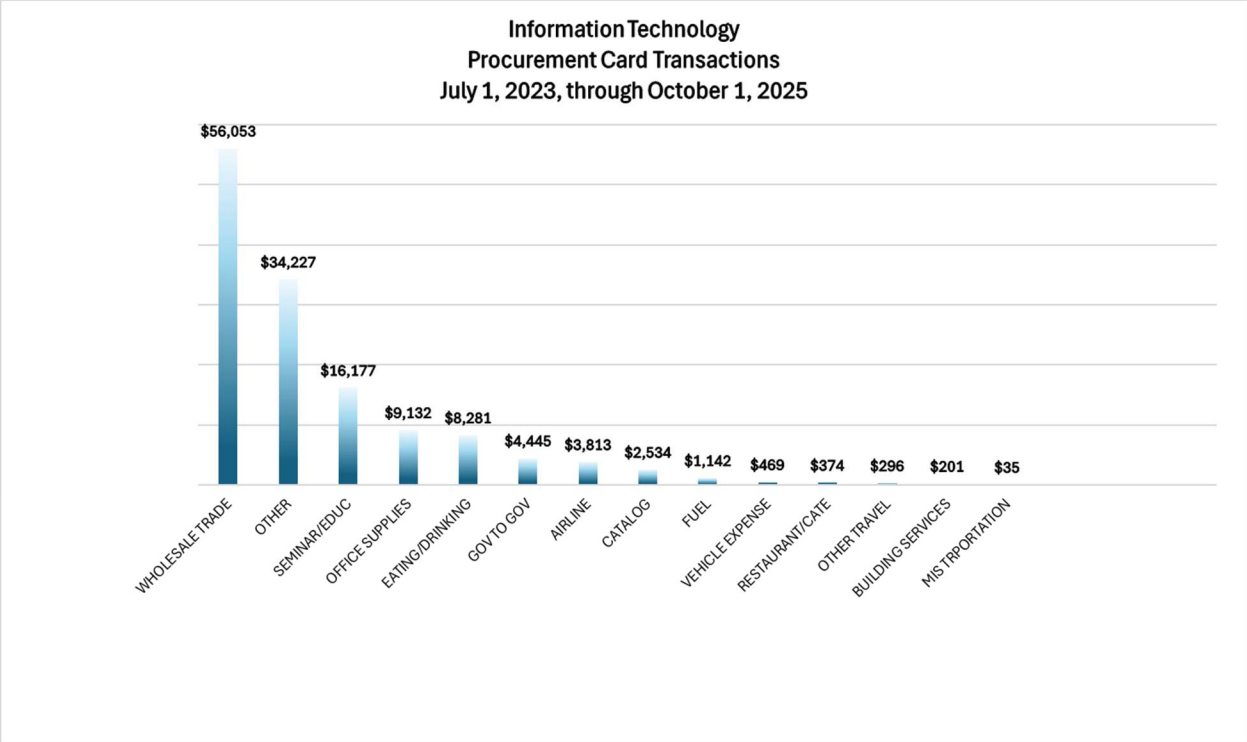
The county's procurement card program was developed to improve efficiencies associated with the procurement process and reduce the costs associated with making purchases and processing vendor payments. The program requires compliance with current statutes and county procurement procedures and is intended to improve the timely delivery of products and services. The Riverside County Purchasing & Fleet Services Department (Purchasing) is responsible for managing and monitoring the overall program. Additionally, Purchasing administers the training required for all program participants, establishes, and communicates rules and guidelines, oversees participants' compliance with the county's procurement policies and procedures, and coordinates the interface between U. S. Bank and the county. Cardholders are required to comply with the Procurement Card Manual as written by Purchasing. Additionally, cardholders must complete the training prior to being provided with a procurement card.

The procurement card policy has controls developed and implemented that are different than traditional credit cards. The controls ensure the cards can be used only for specific types of purchases with established dollar limits. Additionally, approving officials assigned to each cardholder are required to provide prior approval on the purchases. The cardholder is responsible for verifying all purchases once card statement is obtained.

As an integral part of a county department's internal control structure, management within each department is responsible for a system of internal controls that effectively and efficiently performs financial related activities and safeguards assets. The system should provide management with reasonable assurance that assets are properly safeguarded against loss from unauthorized use or theft, and transactions are executed in accordance with management's authorization.

Information Technology has 15 procurement cardholders, as of October 20, 2025. Procurement card expenditures for the period July 1, 2023, through October 31, 2025, included 835 transactions totaling $481,481.

The chart below illustrates Information Technology's procurement card expenditures for the period July 1, 2023, through October 31, 2025, categorized in the following: airline, building services, catalog, eating/drinking, fuel, government to government, MIS transportation, office supplies, other, other travel, restaurant/catering, seminar/education, vehicle expense, wholesale trade.



Objective

To verify the existence and adequacy of internal controls over Information Technology's procurement card management.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of board policies and procedures including:
  - *County of Riverside Procurement Card Program, Procedure Handbook (8/1/2016)*
  - *Information Technology Training and/or Travel Requests (6/18/2024)*
- Interviewed key personnel regarding the department's procurement card process.
- Obtained a list of active procurement cardholders and reviewed transactions for compliance with cardholder agreements.
- Verified proper procurement card issuance.
- Obtained a listing of department employees' time off/vacation/holiday recorded and compared time off recorded dates to transactions dates classified as travel/hotel.

- Analyzed data to identify instances of potential split procurement card transactions and determined that transaction activity was in compliance with cardholder agreements.

- Requested an exit interview checklist and verified it included a procurement card return confirmation.

Finding: None Noted	Priority Level: N/A

Based on the results of our audit, we determined that internal controls over procurement card management provide reasonable assurance that its objective related to this area will be achieved. Reasonable assurance recognizes internal controls have inherent limitations, including cost, mistakes, and intentional efforts to bypass internal controls.

Appendix A: Finding Priority Level Classification

Priority Level 1	Priority Level 2	Priority Level 3
These are audit findings that represent the most critical issues that require immediate attention and pose a significant risk to the department's objectives, compliance, security, financial health, or reputation. They may indicate serious control failures, non-compliance with laws or regulations, significant financial errors, or vulnerabilities with severe potential impact. Immediate corrective measures are necessary to mitigate the risks associated with these findings.	These are audit findings that are important and require timely resolution, but their impact is not as severe as Priority Level 1. They may highlight moderate control weaknesses, areas of non-compliance with internal policies and procedures, or financial discrepancies that are significant but are not critical. While they might not pose an immediate threat, they should be addressed promptly to prevent further escalation or potential negative consequences.	These are audit findings that are less critical and generally have a lower impact on the department's objectives, compliance, or operations. They may include minor control deficiencies, procedural deviations with minimal impact, or non-critical administrative errors. While they may not require immediate attention, they should still be acknowledged and addressed within a reasonable timeframe to ensure ongoing improvement and prevent potential accumulation of minor issues.
Expected Implementation Date of Recommendation* One to three months	**Expected Implementation Date of Recommendation *** Three to six months	**Expected Implementation Date of Recommendation *** Six to twelve months

* Expected completion to implement recommendation date begins after issuance of final audit report.