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

ITEM: 2.10
(ID # 30688)
MEETING DATE:
Tuesday, June 23, 2026

FROM : AUDITOR CONTROLLER

SUBJECT: AUDITOR-CONTROLLER: Internal Audit Report 2026-312: Riverside Treasurer-Tax Collector, Follow-up Audit, [District: All]; [$0]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2026-312: Riverside County Treasurer-Tax Collector, Follow-up Audit.

ACTION:Consent

Ben J. Benoit
Ben J. Benoit, COUNTY AUDITOR-CONTROLLER 6/11/2026

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Perez, seconded by Supervisor Gutierrez 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:	June 23, 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

We completed a follow-up audit of the Riverside County Treasurer-Tax Collector Our audit was limited to reviewing actions taken as of January 13, 2026, to correct findings noted in our original audit report 2025-017 dated August 26, 2025. The original audit report contained seven recommendations, all of which required implementation to help correct the reported findings.

Based on the results of our audit, we found that of the seven recommendations:

- Five of the recommendations were implemented.
- Two of the recommendations were partially implemented.

For an in depth understanding of the original audit report, please refer to Internal Audit Report 2025-017 included as an attachment to this follow-up audit report or it can also be found at https://auditorcontroller.org/divisions/internal-audit/reports.

Impact on Residents and Businesses

Provide an assessment of internal controls over the audited areas.

SUPPLEMENTAL:

Additional Fiscal Information

Not applicable.

ATTACHMENTS:

A: Riverside County Auditor-Controller - Internal Audit Report 2026-312: Riverside County Treasurer-Tax Collector, Follow-up Audit.

Office of Ben J. Benoit

Riverside County Auditor-Controller

Internal Audit Report 2026-312

Follow-up

7 Recommendations

- ✔ 5 Implemented
- ◗ 2 Partially Implemented
- X 0 Not Implemented

Riverside County Treasurer-Tax Collector Follow-up Audit

June 23, 2026

June 23, 2026

Matthew Jennings
Treasurer-Tax Collector
Riverside County Treasurer-Tax Collector
4080 Lemon Street, 4th Floor
Riverside, CA 92501

Subject: **Internal Audit Report 2026-312: Riverside County Treasurer-Tax Collector, Follow-up Audit**

Dear Mr. Jennings:

We completed the follow-up audit of Riverside County Treasurer-Tax Collector. Our audit was limited to reviewing actions taken as of January 13, 2026, to help correct the findings noted in our original audit report 2025-017 dated August 26, 2025.

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 reasonable assurance that our objective, as described in the preceding paragraph, is achieved. Additionally, the standards require that we conduct the audit to provide sufficient, reliable, and relevant evidence to achieve the audit objectives. We believe the audit provides a reasonable basis for our conclusion.

The original audit report contained 7 recommendations, all of which required implementation to help correct the reported findings. Based on the results of our audit, we found that of the 7 recommendations:

- 5 of the recommendations were implemented.
- 2 of the recommendations were partially implemented.

Internal Audit Report 2026-312: Riverside County Treasurer-Tax Collector, Follow-up Audit

A summary of the conditions from the original audit and the results of our review on the status of the implementation of the recommendations are provided in this report. For an in-depth understanding of the original audit, please refer to Internal Audit Report 2025-017 included as "Attachment A" of this audit report along with your department status letter as "Attachment B." You can also find the original audit report at https://auditorcontroller.org/ divisions/internal-audit/reports.

We thank you and your staff for your 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, County Executive Officer
Juan Perez, Chief Operating Officer
Don Kent, Chief Finance Officer
Grand Jury

Table of Contents

Page

Results:

Badge Access Controls 4

Vulnerability Management 5

Attachments:

A. Internal Audit Report 2025-017

B. Status of Findings as Reported by Riverside County Treasurer-Tax Collector on January 13, 2026

Badge Access Controls

Finding 1: Timely Termination of Badge Access

"Office of the Treasurer-Tax Collector Policy A-11, Badge Control Access Policy, states, 'Upon receipt of the ticket the Information Services Technical Support team will place a date and time for the employees account to be disabled. Usually at the end of the day for their last day in the office.'

Three out of 30 (10%) employees separated from the department did not have their badge access deactivated timely. The average time elapsed between employee separation and badge access deactivation as 12 days, with the longest taking 21 days for deactivation and shortest taking 3 days. This is because the current procedures need improvement in conducting periodic reviews of badge access rights to identify and promptly deactivate the badge access. Additionally, during the tax collection season, staff are focused on high-priority operational tasks, which contributed to delays in deactivation of badge access and related communication after badge collection. Not promptly deactivating badges from separated employees can pose significant security and operational risks, including unauthorized entry into restricted areas, exposure of sensitive information, and access to departmental assets. Prompt deactivation of badge access is essential to safeguard sensitive resources, ensure employee safety, and maintain overall departmental security."

Recommendation 1.1

"Deactivate badge access within 24 hours of an employee's separation or transfer from the department."

Current Status 1.1: Implemented

Recommendation 1.2

"Update current procedures to include periodic reviews of badge access rights to ensure timely identification and deactivation of access for separated employees."

Current Status 1.2: Implemented

Recommendation 1.3

"Implement and document periodic reviews of badge access rights to ensure timely identification and deactivation of access for separated employees."

Current Status 1.3: Implemented

Vulnerability Management

Finding 2: Server Upgrades

"National Institute of Standards and Technology's6 NIST SP 800-40, *Procedures for Handling Security Patches,* states, 'Timely patching is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems.'

Five of the Treasurer-Tax Collector's 35 system servers (14%) have not been upgraded to the. supported versions. A process to prioritize and track remediation progress for unresolved vulnerabilities is not maintained, especially vulnerabilities related to using an outdated server operating system. Outdated server operating systems may cause stability issues and contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the applications running on those servers. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences."

Recommendation 2.1

"Develop a process to ensure that the Treasurer-Tax Collector's server operating systems are upgraded in a timely manner before reaching their end of support."

Current Status 2.1: Partially Implemented

The department has undertaken efforts to migrate system servers to supported operating systems; however, as revealed by our follow-up audit, 19 out of the Treasurer-Tax Collector's 29 servers (66%) continue to operate on unsupported versions. This encompasses servers that remain in active use as well as those in varying stages of decommissioning. The department has noted that certain legacy systems must be retained for up to 12 years in adherence to records retention requirements, which impacts the ability to complete timely migrations. Additionally, the complexity and volume of data, along with established encryption protocols, have contributed to extended migration timelines.

Management's Response

"Will continue to make progress and migrate remaining systems to supported operating systems, while taking steps to limit the use of unsupported operating systems."

Recommendation 2.2

"Establish extended security update agreements as needed to maintain coverage during transition periods when upgrades cannot be completed immediately."

Current Status 2.2: Partially Implemented

As stated in Current Status 2.1, 66% of the department's servers operate on unsupported operating systems, including systems that remain in use as well as those in various stages of decommissioning. Extended security update agreements have been established for certain servers, and opportunities remain to expand coverage to all legacy systems that continue to operate.

Management's Response

"Will continue to make progress and migrate remaining systems to supported operating systems, while taking steps to limit the use of unsupported operating systems."

Finding 3: Vulnerability Remediation Tracking

"County of Riverside Information Security Standard Revision v2.0, Section 4.17.4, *Vulnerability Scanning,* states, 'remediate legitimate vulnerabilities per an organizational assessment of risk ...share information obtained from the vulnerability scanning process and control assessments with stakeholders and IT Administrators to help eliminate similar vulnerabilities ...'

Remediation progress for unresolved system vulnerabilities need to be tracked and documented to ensure that remediation steps available for vulnerabilities do not remain unresolved. Additionally, we noted multiple vulnerabilities during the audit period that were outstanding with no documented evidence of remediation progress. See Table B below for the number of total system vulnerabilities by severity as of the fieldwork date, May 21, 2025:

Table B: Number of Total System Vulnerabilities by Severity

Vulnerability Severity	Number of Vulnerabilities	Remediation Response Timeline
Critical	759	7 Days
High	855	14 Days
Medium	492	30 Days

Formal policies and procedures to track severity and remediation progress for unresolved vulnerabilities are not maintained. The absence of tracking the remediation progress impedes the department's ability to closely monitor the implementation status and quickly mitigate any risks posed by the system vulnerabilities."

Recommendation 3.1

"Develop and implement a process to ensure remediation progress for unresolved vulnerabilities is adequately documented, tracked, assigned to personnel, and monitored."

Current Status 3.1: Implemented

Recommendation 3.2

"Enhance the current policies and procedures to develop and implement a process over scanning, severity prioritizing, assigning responsibilities, and tracking progress for the mitigation of unresolved vulnerabilities."

Current Status 3.2: Implemented

Attachment A

Office of Ben J. Benoit

Riverside County Auditor-Controller

Number of Findings & Recommendations

High Risk

2 Findings
- 5 Recommendations

Medium Risk

1 Finding
- 2 Recommendations

Low Risk

0 Findings

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

Internal Audit Report

2025-017

Riverside County Treasurer-Tax Collector Audit

August 26, 2025

COUNTY OF RIVERSIDE
OFFICE OF THE AUDITOR-CONTROLLER

BEN J. BENOIT, AUDITOR-CONTROLLER
TANYA S. HARRIS, DPA, CPA,
ASSISTANT AUDITOR-CONTROLLER

August 26, 2025

Matthew Jennings
Treasurer-Tax Collector
Riverside County Treasurer-Tax Collector
4080 Lemon St. 4th Floor
Riverside, CA 92501

Subject: **Internal Audit Report 2025-017: Riverside County Treasurer-Tax Collector Audit**

Dear Mr. Jennings:

In In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Treasurer-Tax Collector to provide management and the Board of Supervisors with an independent assessment of internal controls over badge access controls, vulnerability management and succession planning.

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.

Internal Audit Report 2025-017: Riverside County Treasurer-Tax Collector 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, Assistant County Executive Officer
Grand Jury

Table of Contents

Page

Executive Summary 4

Results:

Badge Access Controls 6

Vulnerability Management 11

Succession Planning 18

Appendix A: Finding Priority Level Classification 21

Executive Summary

Overview

The Office of the Treasurer-Tax Collector (Treasurer-Tax Collector) is budgeted as one unit and consists of two major divisions: Treasury and Tax Collection. The Treasury Division manages between $14 to $16 billion held in the Treasurer's Pooled Investment Fund on behalf of the county, school districts, special districts, and other discretionary depositors. With three office locations, the Tax Collection Division is responsible for mailing out more than one million secured, unsecured, and supplemental tax bills, collecting over $5.6 billion annually in property taxes, which provides 70% of the county's general-purpose revenue. The Tax Collection Division also enforces collection on tax delinquencies and administers sales of tax-defaulted properties.

The Treasurer-Tax Collector had an adopted budget of $19.89 million for FY 2024/25 and 112 adopted county positions. *County of Riverside, Fiscal Year 2024-25 Adopted Budget Volume 1, 134-135.*

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 badge access controls, vulnerability management, and succession planning. 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

- Separated employee badges need to be deactivated timely.
- Badge policy and procedures need to be enhanced to include periodic reviews of badge access rights.
- Unresolved system vulnerabilities need to be tracked and monitored.
- Server operating systems need to be upgraded to the supported versions.

Audit Scope and Methodology

We conducted the audit from March 5, 2025, through June 10, 2025, for operations from July 1, 2023, through June 5, 2025. Using a risk-based approach, our scope included the following:

- Badge Access Controls
- Vulnerability Management
- Succession Planning

Audit Conclusion

Based on the results of our audit, we determined internal controls over succession planning are functioning as designed to help the Treasurer-Tax Collector achieve its business process objectives. However, we have identified improvement opportunities for internal controls over badge access controls and vulnerability management that can help provide reasonable assurance that the department's objectives relating to these areas will be achieved. Specifically, separated employees' badges need to be deactivated timely, unresolved system vulnerabilities need to be tracked and monitored, and server operating systems need to be upgraded to the supported versions.

Badge Access Control

Background

Access Control Management is a crucial component of information security that involves the establishment, maintenance, and enforcement of policies and procedures to manage access to information systems, resources, and physical facilities within an organization. Access control management plays a vital role in safeguarding sensitive data, maintaining the integrity of systems, and protecting against unauthorized access or breaches. Access extends to physical access control, ensuring that only authorized personnel can enter secure areas or buildings. It is essential for protecting physical assets and sensitive information stored in physical locations.

Badge access controls serve as a fundamental component in establishing and maintaining a secure physical environment within the organization. Badge access controls are essential for regulating and monitoring entry and exit points, aligning with the overarching objective of fortifying the organization's security infrastructure. The utilization of identification badges or electronic access cards contributes to the establishment of robust internal controls, ensuring that access permissions are intricately configured in adherence to organizational security policies and regulatory standards. By objectively assessing the design and functionality of the badge access system, the department can identify any potential vulnerabilities or inefficiencies and determine enhancements that bolster the organization's overall physical security measures.

Below, we detail some examples of instances where lapses in security measures have occurred:

- Aurora, Illinois – Henry Pratt Company Shooting (2019): A terminated employee returned to their former job and opened fire, killing five coworkers and injuring several police officers. The employee had reportedly been fired for disciplinary reasons earlier that day.[1]

- Arlington, Virginia – Reagan National Airport (2013): a former contractor used an unreturned Security Identification Display Area (SIDA) security badge to slip into restricted airport areas, leading to his arrest on trespassing and burglary charges.[2]

- Multnomah County, Oregon (2019): A county employee was dismissed from their job but briefly continued to have access to county records where they were able to obtain the names and social security numbers of 40 clients.[3]

---

[1] "Aurora, Illinois, Gunman Who Fatally Shot 5 Vowed to Kill All His Co-Workers If He Was Fired." NBCNews.Com, NBCUniversal News Group, 29 Apr. 2019.

[2] "Security Badge Breach at Reagan National Airport." NBCWashington.com, NBCUniversal News Group, 24 Apr. 2013.

[3] "Press Release: Multnomah County Reports Security Breach after Employee Termination" | Multnomah County. Multnomah County, 2 July 2019.

These incidents highlight the critical importance of rigorous access control policies. Ensuring badges are promptly deactivated and collected after termination, and continuously monitoring access permissions is essential to prevent such tragedies and maintain security.

Objective

To verify the existence and adequacy of internal controls over the Treasurer-Tax Collector's badge access controls.

Audit Methodology

To accomplish these objectives, we:

- Conducted interviews with key personnel to gain an understanding of the department's badge access control processes and systems.

- Obtained and reviewed relevant badge access control policies and procedures, including Office of the Treasurer-Tax Collector Policy A-11, *Badge Control Access Policy*, and Riverside County Information Security Standard Revision 2.0.

- Obtained a copy of the Treasurer-Tax Collector's organizational chart over badge access control that was effective during the audit period.

- Obtained and reviewed listings of active employees and those separated from the department, as well as employee time-off records during the audit review period.

- Obtained listings of active, deactivated, and temporary badges, including records of assigned, returned, lost, or stolen badges.

- Obtained and reviewed employee access levels, clearance codes, and badge scan logs across Treasurer-Tax Collector facilities.

- Obtained a list of Treasurer-Tax Collector facilities with badge access systems installed.

- Verified whether badge access for separated employees was disabled within 24 hours and supported by sufficient documentation.

- Verified whether badge usage occurred during time off, holidays, outside of normal working hours, or after separation.

- Verified whether any employees had access rights exceeding those of peers in similar roles.

- Verified whether adequate controls exist over loaner and temporary badges, and whether lost or stolen badges were reported and disabled in a timely manner.

- Performed site visits to assess the adequacy of physical security controls, including access points, surveillance, and secure storage areas.

Finding 1: Timely Termination of Badge Access	Priority Level: 1[4]

Office of the Treasurer-Tax Collector Policy A-11, *Badge Control Access Policy*, states, "Upon receipt of the ticket the Information Services Technical Support team will place a date and time for the employees account to be disabled. Usually at the end of the day for their last day in the office."

Three out of 30 (10%) employees separated from the department did not have their badge access deactivated timely. The average time elapsed between employee separation and badge access deactivation as 12 days, with the longest taking 21 days for deactivation and shortest taking 3 days. This is because the current procedures need improvement in conducting periodic reviews of badge access rights to identify and promptly deactivate the badge access. Additionally, during the tax collection season, staff are focused on high-priority operational tasks, which contributed to delays in deactivation of badge access and related communication after badge collection. Not promptly deactivating badges from separated employees can pose significant security and operational risks, including unauthorized entry into restricted areas, exposure of sensitive information, and access to departmental assets. Prompt deactivation of badge access is essential to safeguard sensitive resources, ensure employee safety, and maintain overall departmental security.

Recommendation 1.1

Deactivate badge access within 24 hours of an employee's separation or transfer from the department.

Management's Response

"**Concur**. We have obtained formal authorization from RCIT to assume direct responsibility for managing badge deactivations. This adjustment has enabled us to significantly streamline the workflow, ensuring that all deactivation requests are processed and completed within 24 hours of receipt.

[4] Please see Appendix A (page21) for a description of the finding priority level classifications.

Furthermore, we have revised our badge handling procedures. Instead of pre-scheduling deactivation for a specific time, badges are now permanently removed from the system at the point of deactivation. This enhanced method strengthens overall security and minimizes the potential for unauthorized access."

Actual/estimated Date of Corrective Action: "The corrective action for Recommendation 1.1 will be implemented on July 31, 2025. This update is part of our commitment to improving security and operational efficiency."

Recommendation 1.2

Update current procedures to include periodic reviews of badge access rights to ensure timely identification and deactivation of access for separated employees.

Management's Response

"**Concur**. To address this recommendation, RCIT will begin providing a monthly badge access report to the Treasurer-Tax Collector's (TTC) office. This report will facilitate a comprehensive comparison between the records maintained by TTC and those maintained by County IT.

Following this reconciliation, the Technical Support Team will compile a detailed summary outlining any discrepancies or confirmations between the two datasets. The report will be distributed to the Administration Team, Chief Deputy, Assistant Treasurer-Tax Collector's, and the Treasurer-Tax Collector to ensure leadership remains informed and to maintain alignment between systems.

This measure is part of a broader commitment to improving data integrity, operational efficiency, and internal control effectiveness."

Actual/estimated Date of Corrective Action: "Corrective action for Recommendation 1.2 is scheduled to take effect on July 31, 2025. This action is designed to reinforce internal security controls, ensure timely deactivation of system access, and ·maintain data consistency across records. It reflects our ongoing commitment to safeguarding sensitive information and improving the integrity of badge management procedures."

Recommendation 1.3

Implement and document periodic reviews of badge access rights to ensure timely identification and deactivation of access for separated employees.

Management's Response

"**Concur**. To address this recommendation, TTC will begin receiving a monthly report from RCIT. This report will support regular reviews by allowing for thorough comparison between records maintained by TTC and those maintained by County IT.

In addition, every 60 days the Administration Team will conduct an independent audit to review alignment between the two data sources and ensure ongoing compliance. This process reinforces internal controls and strengthens timely access termination procedures."

Actual/estimated Date of Corrective Action: "In accordance with the planned corrective measures, implementation for Recommendation 1.3 will commence on July 31, 2025, to ensure timely and consistent deactivation of badge access for separated employees through periodic reviews and strengthened oversight protocols."

Vulnerability Management

Background

Vulnerability management is the process of identifying, assessing, and resolving known published vulnerabilities in the enterprise information system. Vulnerability assessments are meant to discover and prioritize vulnerabilities, ensuring that organizations can address the most critical issues first. This process involves updating a vulnerability database and scanning the enterprise network and system for vulnerabilities, assessing the risk associated with each, and recommending strategies to remediate or mitigate the identified weaknesses that could result in threats to enterprise security, which can manifest in various forms, including malware, ransomware, phishing attacks, unauthorized access, and denial-of-service attacks. Security controls such as timely system upgrades, regular scanning, prioritization of application, firewalls, intrusion detection prevention systems, and access controls are tools to mitigate these threats.

Patch management is a critical component of maintaining a secure network infrastructure. It involves regularly updating software, operating systems, and applications to address known vulnerabilities and improve overall system stability. Effective patch management processes ensure that timely and appropriate patches are applied to mitigate the risk of exploitation by cyber threat actors.

Incident response is critical, involving constant monitoring of malicious codes and attempted breaches by cyber threat actors exploiting system vulnerabilities. This process strategically neutralizes threats by blocking them or quarantining infected files or applications, acting as a detective control, while vulnerability assessment and patch management serve as preventive controls. Preventive controls are prioritized to minimize the frequency of repetitive threat

Objective

To verify the existence and adequacy of internal controls over the Treasurer-Tax Collector's vulnerability management of information systems.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of Riverside County Information Security Standard Revision 2.0.

- Interviewed key personnel and reviewed the Treasurer-Tax Collector's procedures over vulnerability management.

- Verified whether adequate segregation of duties is in place relating to vulnerability management.

- Obtained the department's vulnerability management plan and verified the existence of adequate insurance coverage, vulnerability assessments, patch management processes, and incident response plans.

- Obtained the department's vulnerability assessment report and verified whether vulnerabilities are tracked and resolved timely.

- Obtained the department's incident response report and verified whether threats are neutralized timely.

- Obtained a listing of department applications and verified whether an adequate patch management system is used and applications are assigned risk ratings.

Finding 2: Server Upgrades	Priority Level: 2[5]

National Institute of Standards and Technology's[6] NIST SP 800-40, *Procedures for Handling Security Patches*, states, "Timely patching is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems."

Five of the Treasurer-Tax Collector's 35 system servers (14%) have not been upgraded to the supported versions. A process to prioritize and track remediation progress for unresolved vulnerabilities is not maintained, especially vulnerabilities related to using an outdated server operating system. Outdated server operating systems may cause stability issues and contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the applications running on those servers. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences.

Recommendation 2.1

Develop a process to ensure that the Treasurer-Tax Collector's server operating systems are upgraded in a timely manner before reaching their end of support.

---

[5] Please see Appendix A (page21) for a description of the finding priority level classifications.

[6] NIST is a federal agency within the US Department of Commerce whose standards and guidelines on security and privacy are considered authoritative references in designing and implementing security measures, including access control policies. Their standards are critical for ensuring the integrity, confidentiality, and availability of information systems, making them a reputable source for guiding security practices.

Management's Response

"**Concur**. TTC has a formalized and ongoing server upgrade strategy designed to ensure optimal system performance and robust security. As part of our modernization efforts, we are actively phasing out legacy servers and migrating data to a secure, up-to-date infrastructure.

Currently, a small number of legacy servers remain in operation. These systems, some dating back to 2012, are fully isolated from internet access and present minimal risk. Over the past year, we have made substantial progress in transferring data from these servers to a new Remittance Processing depository. Migration is on track, with all data now transferred through the current year. Once final validation is complete, the 2012 servers will be decommissioned in accordance with IT asset management and decommissioning protocols.

Additionally, we have initiated plans to replace 2019 servers, which remain under support through 2029, with a newer 2025 server platform. Although technical issues have temporarily delayed migration to the 2025 environment, new hardware has been procured, and stabilization efforts are underway. A full cutover will proceed upon resolution of these issues, at which time all systems will be operating on our most current and secure infrastructure.

This staged transition approach ensures continued data integrity, enhanced system reliability, and full alignment with industry best practices and security standards."

Actual/estimated Date of Corrective Action: "Although technical issues have temporarily delayed implementation, remediation efforts are actively underway. The full transition and decommissioning process will be finalized by October 31, 2025. This corrective action reinforces our commitment to maintaining data integrity, strengthening infrastructure resiliency, and aligning with industry standards for system security and operational excellence."

Recommendation 2.2

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

Management's Response

"**Concur**. TTC concurs with this recommendation and recognizes the importance of maintaining extended support coverage during infrastructure transition periods. Our oldest actively supported servers, primarily from 2019, are currently covered under extended support agreements through 2029, ensuring the continued receipt of critical patches and security protections.

There are a small number of legacy servers, specifically units originally deployed in 2012, which surpassed their extended support dates. These systems are fully isolated from internet access and are confined strictly to internal operations. This containment approach significantly mitigates security exposure and ensures they do not pose a threat to broader network infrastructure.

Over the past year, the TTC has actively advanced its infrastructure modernization efforts by transferring data from legacy servers, specifically those dated back to 2012, to a secure Remittance Processing depository. Significant progress has been achieved, with all relevant data successfully migrated through the current year. Upon completion and validation of the final phase, the 2012 servers will be fully decommissioned in accordance with established IT asset management and decommissioning protocols.

In addition, the set of servers from 2019, although are still supported, are also slated for replacement. To facilitate this upgrade, new hardware has already been procured for deployment within the 2025 server environment. However, technical challenges encountered have temporarily delayed the transition. Until these issues are resolved and the 2025 environment is stabilized, we are unable to proceed with the cutover. Once the 2025 environment is stable and fully operational, we will complete the migration process. At that time, all our infrastructure will be running in the most up-to-date server environment, ensuring improved performance, security, and long-term support.

TTC is actively migrating all data and services from outdated server infrastructure to a secure, modern database environment. This effort is being carried out in accordance with our established IT modernization strategy. Once the migration is complete and validated, all legacy servers will be fully decommissioned in line with our IT asset management policies and decommissioning protocols.

This initiative reflects TTC's commitment to infrastructure resiliency, secure operations, and alignment with industry standards. Extended update agreements will continue to be utilized as needed to ensure coverage throughout these strategic upgrades."

Actual/estimated Date of Corrective Action: "To ensure continued coverage and minimize risk during transition periods, we will maintain appropriate extended support agreements where necessary. The corrective action will be fully implemented by October 31, 2025, in alignment with our IT modernization strategy and infrastructure upgrade timelines."

Finding 3: Vulnerability Remediation Tracking | Priority Level: 1[7]

County of Riverside Information Security Standard Revision v2.0, Section 4.17.4, *Vulnerability Scanning,* states, "remediate legitimate vulnerabilities per an organizational assessment of risk... share information obtained from the vulnerability scanning process and control assessments with stakeholders and IT Administrators to help eliminate similar vulnerabilities..."

Remediation progress for unresolved system vulnerabilities need to be tracked and documented to ensure that remediation steps available for vulnerabilities do not remain unresolved. Additionally, we noted multiple vulnerabilities during the audit period that were outstanding with no documented evidence of remediation progress. See Table B below for the number of total system vulnerabilities by severity as of the fieldwork date, May 21, 2025:

Table B: Number of Total System Vulnerabilities by Severity

Vulnerability Severity	Number of Vulnerabilities	Remediation Response Timeline[8]
Critical	759	7 Days
High	855	14 Days
Medium	492	30 Days

Formal policies and procedures to track severity and remediation progress for unresolved vulnerabilities are not maintained. The absence of tracking the remediation progress impedes the department's ability to closely monitor the implementation status and quickly mitigate any risks posed by the system vulnerabilities.

Recommendation 3.1

Develop and implement a process to ensure remediation progress for unresolved vulnerabilities is adequately documented, tracked, assigned to personnel, and monitored.

Management's Response

"**Concur**. Following the receipt of the Rapid7 report, TTC has initiated the development of a comprehensive remediation plan to address all systems identified as outdated or non-compliant. This effort includes prioritizing updates and ensuring that all required patches are thoroughly tested for compatibility across TTC's diverse range of systems and applications.

---

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

[8] County of Riverside Information Security Standard Revision v2.0, Section 4.20.2, Flaw Remediation, establishes timelines for which security-relevant software and firmware updates are to be installed upon vulnerability identification.

To ensure accountability and effective oversight, TTC will implement a structured process for managing vulnerabilities. Each vulnerability identified in the monthly Rapid7 report will be assigned to a responsible team or individual, with clear timelines for resolution. A centralized tracking report will be created to document key details such as the assigned owner, status updates, and the date each issue is resolved."

Actual/estimated Date of Corrective Action: "October 31, 2025."

Recommendation 3.2

Enhance the current policies and procedures to develop and implement a process over scanning, severity prioritizing, assigning responsibilities, and tracking progress for the mitigation of unresolved vulnerabilities.

Management's Response

"**Concur**. TTC's Vulnerability Management Policy has recently been updated to better align with current staffing levels and operational timelines. These revisions ensure that vulnerability remediation efforts remain achievable and effective within existing resource constraints, while still maintaining a strong security posture.

Our remediation strategy prioritizes vulnerabilities based on their severity. Critical vulnerabilities will be addressed first to mitigate the most significant risks to our systems and data. Once critical issues are resolved, our teams will proceed to address high-severity vulnerabilities, followed by those of medium and lower priority, in a structured and timely manner.

The TTC takes a strategic and cautious approach when deploying software patches, with particular attention given to critical operational hours and service timelines. Before any patch is implemented, we carefully assess the potential impact on essential systems to avoid introducing risks that could disrupt transit operations or compromise service reliability.

To further mitigate potential issues, the TTC follows a practice of delaying patch deployment until updates have been thoroughly tested and verified by trusted external sources or vendors. This ensures compatibility with our existing infrastructure and significantly reduces the risk of deploying unproven patches that could inadvertently impact mission-critical systems.

This approach allows the TTC to balance security with operational stability, ensuring that necessary updates are applied without compromising the availability or integrity of transit services, especially during periods when the organization is most operationally vulnerable. By

aligning patch management with our delivery priorities, we are better able to maintain both system security and public trust.

We will continue to closely monitor the monthly Rapid 7 vulnerability reports provided by RCIT. These reports are essential in helping us identify and respond to security issues across TTC's infrastructure. For each flagged item, we will track its status through to resolution, document the actions taken, and include detailed comments within the report to maintain a clear record of progress.

This process not only supports accountability and transparency but also reinforces TTC's commitment to proactively managing cybersecurity risks and maintaining the integrity of our IT systems."

Actual/estimated Date of Corrective Action: "October 31, 2025."

Succession Planning

Background

Succession planning is a strategic process crucial for ensuring the continuity of leadership within an organization. This process involves identifying and developing internal employees who have the potential to fill key leadership positions. Succession planning is not just about filling vacancies. It is about preparing the county for the future by maintaining a pipeline of capable leaders who can drive the organization forward. It helps maintain the leadership continuity, preserves institutional knowledge, and ensures a smooth transition of critical functions and services provided by key positions within the organization.

All members of management are responsible for individual succession planning efforts. Department and division managers are responsible for implementing the program within their respective areas and should coordinate with Human Resources personnel for effectiveness of succession planning efforts for key leadership positions.

The primary objective of a succession plan is to limit the potential challenges to unexpected terminations or departures from an organization. According to the Government Finance Officers Association[9] (GFOA), "A successful succession plan should place a high priority on planning for a smooth change in such positions. Key components of an integrated succession management approach include workforce planning, succession planning, knowledge management practices, and recruitment and retention practices."

In the absence of formal guidance over succession planning, the focus of our audit was to ensure that the Treasurer-Tax Collector had adequate, documented policies and procedures in the event of management or personnel turnover. Specifically, we reviewed the department's prioritization of critical positions to the department's ongoing operations, key objectives, and critical system applications used. In addition to reviewing documented policies and procedures associated with these attributes, we also focused on whether the department had established training programs to ensure knowledge is transferred among personnel so, in the event of turnover, the lapse in business continuity is minimized.

The following flowchart illustrates the Government Finance Officers Association's 10 Steps to Succession Planning[10] that will help an organization retain key talent and find skilled employees to replace staff members who move on:

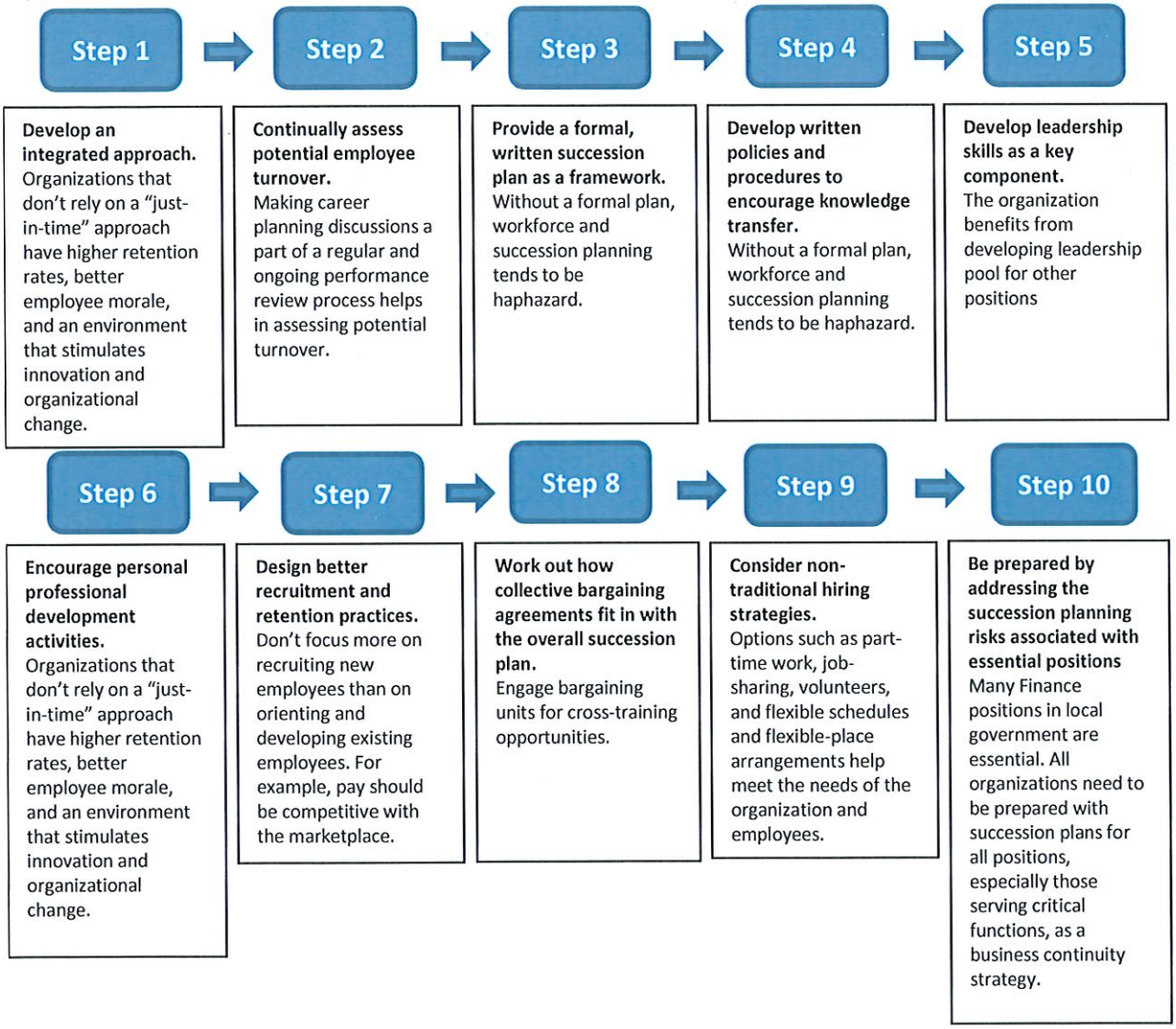
---

[9] Key issues in succession planning. Government Finance Officers Association. (2011, February 28). https://www.gfoa.org/materials/key-issues-in-succession-planning

[10] *10 Steps to Succession Planning*. Government Finance Officers Association. (2022, February). https://www.gfoa.org/materials/gfr222-10steps

Flowchart 1: 10 Steps to Succession Planning

"Succession planning has gotten even more challenging in recent years, given a changing job market, shorter employee tenure, and COVID-19 job turnover-which means that governments should make it an even higher priority. GFOA's 10 steps to succession planning will help your organization retain key talent and find skilled employees to replace staff members who move on."[11]



[11] *10 Steps to Succession Planning*. Government Finance Officers Association. (2022, February). https://www.gfoa.org/materials/gfr222-10steps

Objective

To verify the existence and adequacy of internal controls over the Treasurer-Tax Collector's succession planning process.

Audit Methodology

To accomplish these objectives, we:

- Conducted interviews and performed walk-throughs with department personnel responsible for succession planning.
- Obtained an understanding of relevant continuity plans, including desk procedures, job aids and transfer strategies.
- Obtained a listing of employees that separated from the department during the audit review period.
- Identified positions critical to department operations and positions with the high turnover rate.
- Identified key, transferable knowledge and essential systems tied to identified positions.
- Assessed adequacy of succession planning procedures by verifying whether critical roles and positions with higher turnover have established processes for continuity and effective coverage.

Finding: None Noted

Based on the results of our audit, we determined that internal controls over succession planning 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.

Attachment B

MATTHEW JENNINGS
County of Riverside Treasurer - Tax Collector

Giovane Pizano
Assistant Treasurer

Melissa Johnson
Assistant Tax Collector

The following are the current status of the reported findings and planned corrective actions contained in Internal Audit Report 2025-017: Riverside County Treasurer-Tax Collector.

1/13/2026

Authorized Signature **Date**

Finding 1: Timely Termination of Badge Access

"Office of the Treasurer-Tax Collector Policy A-11, Badge Control Access Policy, states, 'Upon receipt of the ticket the Information Services Technical Support team will place a date and time for the employees account to be disabled. Usually at the end of the day for their last day in the office.'

Three out of 30 (10%) employees separated from the department did not have their badge access deactivated timely. The average time elapsed between employee separation and badge access deactivation as 12 days, with the longest taking 21 days for deactivation and shortest taking 3 days. This is because the current procedures need improvement in conducting periodic reviews of badge access rights to identify and promptly deactivate the badge access. Additionally, during the tax collection season, staff are focused on high-priority operational tasks, which contributed to delays in deactivation of badge access and related communication after badge collection. Not promptly deactivating badges from separated employees can pose significant security and operational risks, including unauthorized entry into restricted areas, exposure of sensitive information, and access to departmental assets. Prompt deactivation of badge access is essential to safeguard sensitive resources, ensure employee safety, and maintain overall departmental security."

Current Status

Reported Finding Corrected? [X] **Yes** [ ] **No**

Recommendation 1.1

"Deactivate badge access within 24 hours of an employee's separation or transfer from the department."

Management Reply

"**Concur.** We have obtained formal authorization from RCIT to assume direct responsibility for managing badge deactivations. This adjustment has enabled us to significantly streamline the workflow, ensuring that all deactivation requests are processed and completed within 24 hours of receipt.

Furthermore, we have revised our badge handling procedures. Instead of pre-scheduling deactivation for a specific time, badges are now permanently removed from the system at the point of deactivation. This enhanced method strengthens overall security and minimizes potential for unauthorized access."

Actual/Estimated Date of Corrective Action: July 31, 2025

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

We have received formal authorization from RCIT to assume direct responsibility for managing badge deactivations. This change has enabled us to significantly streamline the process, ensuring that all deactivation requests are completed within 24 hours of receipt.

Due to occasional staffing constraints, some deactivations may need to be pre-scheduled for a specific time. All employee badges are submitted to TTC Human Resources prior to an employee's departure. In instances where an employee is separated from employment while off-site, a ticket is submitted and the badge is deactivated on the same day.

All badge-related tickets are processed within a 24-hour timeframe, including those requiring scheduled deactivation, which fully removes access to all TTC facilities. When a badge must be deactivated urgently, the team will subsequently delete the badge record immediately at the earliest practical opportunity.

Recommendation 1.2

"Update current procedures to include periodic reviews of badge access rights to ensure timely identification and deactivation of access for separated employees."

Management Reply

"**Concur**. To address this recommendation, RCIT will begin providing a monthly badge access report to the Treasurer-Tax Collector's (TTC) office. This report will facilitate a comprehensive comparison between the records maintained by TTC and those maintained by County IT.

Following this reconciliation, the Technical Support Team will compile a detailed summary outlining any discrepancies or confirmations between the two datasets. The report will be distributed to the Administration Team, Chief Deputy, Assistant Treasurer-Tax Collector's, and the Treasurer-Tax Collector to ensure leadership remains informed and to maintain alignment between systems.

This measure is part of a broader commitment to improving data integrity, operational efficiency, and internal control effectiveness."

Actual/Estimated Date of Corrective Action: July 31, 2025

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

The Treasurer–Tax Collector has met the requirement as outlined. Instead of relying solely on reports provided by RCIT, our office has been granted the ability to independently generate the required access control reports. Badge access rights are reviewed every 60 days for compliance

An internal report is produced and reconciled against the dataset derived from trouble tickets submitted for individuals with system access, specifically reviewing all access modifications and terminations. This reconciliation ensures that access changes are appropriately documented and executed within the required timeframe.

In the event that a discrepancy is identified during the review period, the Technical Support Team is required to provide a written explanation documenting the cause and resolution.

Recommendation 1.3

"Implement and document periodic reviews of badge access rights to ensure timely identification and deactivation of access for separated employees."

Management Reply

"**Concur**. To address this recommendation, TTC will begin receiving a monthly report from RCIT. This report will support regular reviews by allowing for thorough comparison between records maintained by TTC and those maintained by County IT.

In addition, every 60 days the Administration Team will conduct an independent audit to review alignment between these two data sources and ensure ongoing compliance. This process reinforces internal controls and strengthens timely access termination procedures."

Actual/Estimated Date of Corrective Action: July 31, 2025

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

The Administrative Unit perform an independent review of the reports to confirm that the Technical Support Team is in compliance with badge and system access control requirements.

Finding 2: Server Upgrades

"National Institute of Standards and Technology's6 NIST SP 800-40, *Procedures for Handling Security Patches,* states, 'Timely patching is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems.'

Five of the Treasurer-Tax Collector's 35 system servers (14%) have not been upgraded to the. supported versions. A process to prioritize and track remediation progress for unresolved vulnerabilities is not maintained, especially vulnerabilities related to using an outdated server operating system. Outdated server operating systems may cause stability issues and contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the applications running on those servers. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences.

Current Status

Reported Finding Corrected? [X] **Yes** [ ] **No**

Recommendation 2.1

"Develop a process to ensure that the Treasurer-Tax Collector's server operating systems are upgraded in a timely manner before reaching their end of support."

Management Reply

"**Concur.** TTC has a formalized and ongoing server upgrade strategy designed to ensure optimal system performance and robust security. As part of our modernization efforts, we are actively phasing out legacy servers and migrating data to a secure, up-to-date infrastructure.

Currently, a small number of legacy servers remain in operation. These systems, some dating back to 2012, are fully isolated from internet access and present minimal risk. Over the past year, we have made substantial progress in transferring data from these servers to a new Remittance Processing depository. Migration is on track, with all data now transferred through the current year. Once final validation is complete, the 2012 servers will be decommissioned in accordance with IT asset management and decommissioning protocols.

Additionally, we have initiated plans to replace 2019 servers, which remain under support through 2029, with a newer 2025 server platform. Although technical issues have temporarily delayed migration to the 2025 environment, new hardware has been procured, and stabilization efforts are underway. A full cutover will proceed upon resolution of these issues, at which time all systems will be operating on our most current and secure infrastructure.

This staged transition approach ensures continued data integrity, enhanced system reliability, and full alignment with industry best practices and security standards."

Actual/Estimated Date of Corrective Action: October 31, 2025

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

TTC has continued to acknowledge the importance of maintaining extended support coverage during periods of infrastructure transition and has a process in place to ensure that systems are upgraded in a timely manner Our oldest actively supported servers, primarily deployed in 2019, remain under extended support agreements through 2029. This ensures the continued availability of critical security updates and patches.

Over the past several months, it has been determined that the data residing on the 2012 servers cannot be migrated to another server by our vendor. Due to Revenue and Taxation retention requirements, TTC is obligated to maintain access to this data for up to an additional five years in the event of a records request. As an added precaution, the servers have been further isolated and powered down, remaining offline until such time as the data is required. These servers have been updated to the most recent Microsoft Server patches available for that platform. The data hosted on these servers is fully encrypted, protected behind the firewall and entirely isolated from internet access while in use.

TTC continues to make substantial progress in advancing its infrastructure modernization efforts. Data from legacy servers has been actively migrated to a secure Remittance Processing depository. All relevant data through the current year has been successfully transferred. During this process, additional storage capacity was required due to significant file growth, which had temporarily impacted transfer performance. The project is now proceeding as planned, with an anticipated completion date of March 31, 2026.
At present, all core infrastructure is operating on the most up-to-date server environment, providing enhanced performance, security, and long-term support.

Recommendation 2.2

"Establish extended security update agreements as needed to maintain coverage during transition periods when upgrades cannot be completed immediately."

Management Reply

"**Concur.** TTC concurs with this recommendation and recognizes the importance of maintaining extended support coverage during infrastructure transition periods. Our oldest actively supported servers, primarily from 2019, are currently covered under extended support agreements through 2029, ensuring the continued receipt of critical patches and security protections.

There are a small number of legacy servers, specifically units originally deployed in 2012, which surpassed their extended support dates. These systems are fully isolated from internet access and are confined strictly to internal operations. This containment approach significantly mitigates security exposure and ensures they do not pose a threat to broader network infrastructure.

Over the past year, the TTC has actively advanced its infrastructure modernization efforts by transferring data from legacy servers, specifically those dated back to 2012, to a secure Remittance Processing depository. Significant progress has been achieved, with all relevant data successfully migrated through the current year. Upon completion and validation of the final phase, the 2012 servers will be fully decommissioned in accordance with established IT asset management and decommissioning protocols.

In addition, the set of servers from 2019, although are still supported, are also slated for replacement. To facilitate this upgrade, new hardware has already been procured for deployment within the 2025 server environment. However, technical challenges encountered have temporarily delayed the transition. Until these issues are resolved and the 2025 environment is stabilized, we are unable to proceed with the cutover. Once the 2025 environment is stable and fully operational, we will complete the migration process. At that time, all our infrastructure will be running in the most up-to-date server environment, ensuring improved performance, security, and long-term support.

TTC is actively migrating all data and services from outdated server infrastructure to a secure, modern database environment. This effort is being carried out in accordance with our established IT modernization strategy. Once the migration is complete and validated, all legacy servers will be fully decommissioned in line with our IT asset management policies and decommissioning protocols.

This initiative reflects TTC's commitment to infrastructure resiliency, secure operations, and alignment with industry standards. Extended update agreements will continue to be utilized as needed to ensure coverage throughout these strategic upgrades."

Actual/Estimated Date of Corrective Action: October 31, 2025

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

A limited number of legacy servers, specifically those originally deployed in 2012, have exceeded their extended support lifecycle. The data hosted on these servers is fully encrypted, protected behind the firewall, and entirely isolated from internet access. These systems are restricted to internal operations only, significantly reducing security exposure and mitigating any risk to the broader network infrastructure. Additionally, these servers have been updated to the most recent Microsoft Server patches available for that platform.

Over the past several months, it has been determined that the data residing on the 2012 servers cannot be migrated to another server by our vendor. Due to Revenue and Taxation retention requirements, TTC is obligated to maintain access to this data for up to an additional five years in the event of a records request. As an added precaution, the servers have been further isolated and powered down, remaining offline until such time as the data is required.

At present, all core infrastructure is operating on the most up-to-date server environment, providing enhanced performance, security, and long-term support.

Finding 3: Vulnerability Remediation Tracking

"County of Riverside Information Security Standard Revision v2.0, Section 4.17.4, *Vulnerability Scanning,* states, "remediate legitimate vulnerabilities per an organizational assessment of risk ...share information obtained from the vulnerability scanning process and control assessments with stakeholders and IT Administrators to help eliminate similar vulnerabilities ... "

Remediation progress for unresolved system vulnerabilities needs to be tracked and documented to ensure that remediation steps available for vulnerabilities do not remain unresolved. Additionally, we noted multiple vulnerabilities during the audit period that were outstanding with no documented evidence of remediation progress. See Table B below for the number of total system vulnerabilities by severity as of the fieldwork date, May 21, 2025:

Table B: Number of Total System Vulnerabilities by Severity

Vulnerability Severity	Number of Vulnerabilities	Remediation Response Timeline
Critical	759	7 Days
High	855	14 Days
Medium	492	30 Days

Formal policies and procedures to track severity and remediation progress for unresolved vulnerabilities are not maintained. The absence of tracking the remediation progress impedes the department's ability to closely monitor the implementation status and quickly mitigate any risks posed by the system vulnerabilities.

Current Status

Reported Finding Corrected? [X] **Yes** [ ] **No**

Recommendation 3.1

"Develop and implement a process to ensure remediation progress for unresolved vulnerabilities is adequately documented, tracked, assigned to personnel, and monitored."

Management Reply

"Concur. Following the receipt of the Rapid7 report, TTC has initiated the development of a comprehensive remediation plan to address all systems identified as outdated or non-compliant. This effort includes prioritizing updates and ensuring that all required patches are thoroughly tested for compatibility across TTC's diverse range of systems and applications.

To ensure accountability and effective oversight, TTC will implement a structured process for managing vulnerabilities. Each vulnerability identified in the monthly Rapid7 report will be assigned to a responsible team or individual, with clear timelines for resolution. A centralized tracking report will be created to document key details such as the assigned owner, status updates, and the date each issue is resolved."

Actual/Estimated Date of Corrective Action: October 31, 2025

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

Following receipt of the Rapid7 report, TTC initiated the development of a comprehensive remediation plan to address all systems identified as outdated or non-compliant. This plan includes prioritizing remediation activities and ensuring that all required patches and configuration changes are thoroughly tested for compatibility across TTC's diverse systems and applications prior to deployment.

To ensure accountability and effective oversight, TTC has implemented a structured vulnerability management process. Each vulnerability identified in the monthly Rapid7 report is assigned to a designated team or individual responsible for investigation, remediation, or formal risk disposition.

All findings are documented directly within the Rapid7 report upon completion of remediation or investigation. By way of example, one item identified in the Rapid7 report for this audit related to the configuration setting "Set an account lockout threshold for Microsoft Windows," which affected 129 machines. Following a detailed review, TTC determined that this control is not required for current operational needs and that associated risks have been mitigated through alternative safeguards.

Specifically, user access is restricted to predefined timeframes aligned with job responsibilities, and access is closely monitored. In situations where a user account becomes locked and the service desk is unable to immediately respond; users are permitted to regain access after a 30-minute lockout period by re-entering their correct credentials. This approach balances security requirements with operational continuity while maintaining an acceptable risk posture.

Recommendation 3.2

"Enhance the current policies and procedures to develop and implement a process over scanning, severity prioritizing, assigning responsibilities, and tracking progress for the mitigation of unresolved vulnerabilities."

Management Reply

"Concur. TTC's Vulnerability Management Policy has recently been updated to better align with current staffing levels and operational timelines. These revisions ensure that vulnerability remediation efforts remain achievable and effective within existing resource constraints, while still maintaining a strong security posture.

Our remediation strategy prioritizes vulnerabilities based on their severity. Critical vulnerabilities will be addressed first to mitigate the most significant risks to our systems and data. Once critical issues are resolved, our teams will proceed to address high-severity vulnerabilities, followed by those of medium and lower priority, in a structured and timely manner.

The TTC takes a strategic and cautious approach when deploying software patches, with particular attention given to critical operational hours and service timelines. Before any patch is implemented, we carefully assess the potential impact on essential systems to avoid introducing risks that could disrupt transit operations or compromise service reliability.

To further mitigate potential issues, the TTC follows a practice of delaying patch deployment until updates have been thoroughly tested and verified by trusted external sources or vendors. This ensures compatibility with our existing infrastructure and significantly reduces the risk of deploying unproven patches that could inadvertently impact mission-critical systems.

This approach allows the TTC to balance security with operational stability, ensuring that necessary updates are applied without compromising the availability or integrity of transit services, especially

during periods when the organization is most operationally vulnerable. By aligning patch management with our delivery priorities, we are better able to maintain both system security and public trust.

We will continue to closely monitor the monthly Rapid 7 vulnerability reports provided by RCIT. These reports are essential in helping us identify and respond to security issues across TTC's infrastructure. For each flagged item, we will track its status through to resolution, document the actions taken, and include detailed comments within the report to maintain a clear record of progress.

This process not only supports accountability and transparency but also reinforces TTC's commitment to proactively managing cybersecurity risks and maintaining the integrity of our IT systems."

Actual/Estimated Date of Corrective Action: October 31, 2025

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

Prior to this audit, TTC was not consistently receiving the Rapid7 vulnerability reports due to an incorrect configuration. This issue has since been remediated. TTC is now enrolled in a structured monthly reporting cycle and receives the Rapid7 report on the Monday preceding the "Super Tuesday" patch releases. This timing allows staff to review all relevant vulnerability information prior to the deployment of new patches.

In addition to receiving the monthly Rapid7 reports, TTC has met with RCIT to conduct additional Rapid7 training. During these sessions, RCIT provided training on the broader capabilities of the Rapid7 application, enabling TTC staff to independently perform vulnerability scans as needed rather than relying solely on the monthly report. This enhancement allows TTC to proactively identify and address vulnerabilities that may impact the department at any time.

TTC will continue to delay patch deployment until updates have been adequately tested and validated through trusted external sources or vendors. This approach ensures compatibility with the existing infrastructure and significantly reduces the risk of deploying unproven patches that could inadvertently impact mission-critical systems. Accordingly, patches are scheduled for deployment on the Sunday two weeks following release, allowing sufficient time for testing and verification.

TTC monitors the monthly Rapid7 vulnerability reports provided by RCIT. Action items from each report are assigned to specific team members to ensure accountability and timely remediation. The majority of items identified in the May report have been resolved. Exceptions include vulnerabilities that must be maintained due to Revenue and Taxation Code requirements, as well as one item for which TTC has determined that the operational risk does not outweigh the potential loss of productivity associated with implementing a Windows timeout lock. This risk has been formally acknowledged and accepted by TTC, and RCIT has been informed.

TTC will continue to review Rapid7 reports on a monthly basis and remediate vulnerabilities affecting critical systems in a timely manner, ensuring ongoing compliance with security and operational requirements.