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

ITEM: 2.12
(ID # 28134)
MEETING DATE:
Tuesday, June 24, 2025

FROM : AUDITOR CONTROLLER

SUBJECT: AUDITOR-CONTROLLER: Internal Audit Report 2025-312: Riverside County Information Technology Department, Follow-up Audit, [District: All]; [$0]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2025-312: Riverside County Information Technology Department, Follow-up Audit.

ACTION:Consent

Ben J. Benoit, COUNTY AUDITOR-CONTROLLER 6/9/2025

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Spiegel, seconded by Supervisor Medina 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 24, 2025
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 Riverside County Information Technology. Our audit was limited to reviewing actions taken as of February 24, 2025, to correct findings noted in our original audit report 2024-009 dated June 11, 2024. The original audit report contained 14 recommendations, all of which required implementation to help correct the reported findings.

Based on the results of our audit, we found that of the 14 recommendations

- 10 of the recommendations were implemented.
- 4 of the recommendations were partially implemented.

For an in-depth understanding of the original audit, please refer to Internal Audit Report 2024-009 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 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 - Internal Audit Report 2025-312: Riverside County Information Technology Department, Follow-up Audit

Office of Ben J. Benoit

Riverside County Auditor-Controller

Internal Audit Report 2025-312

Follow-up

14 Recommendations

- ✔ 10 Implemented
- ▶ 4 Partially Implemented
- X 0 Not Implemented

Riverside County Information Technology Department, Follow-up Audit

June 24, 2025

June 24, 2025

Martin Perez
Interim Chief Technology Officer
Riverside County Information Technology
3450 14th Street
Riverside, CA 92501

Subject: **Internal Audit Report 2025-312: Riverside County Information Technology Department, Follow-up Audit**

Dear Mr. Perez:

We completed the follow-up audit of Riverside County Information Technology. Our audit was limited to reviewing actions taken as of February 24, 2025, to help correct the findings noted in our original audit report 2024-009 dated June 11, 2024.

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 14 recommendations, all of which required implementation to help correct the reported findings. Based on the results of our audit, we found that of the 14 recommendations:

- 10 of the recommendations were implemented.
- 4 of the recommendations were partially implemented.

Internal Audit Report 2025-312: Riverside County Information Technology Department, 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 2024-009 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 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, County Executive Officer
Juan Perez, Chief Operating Officer
Grand Jury

Table of Contents

Access Controls

Finding 1: Termination of Badge Access

"County of Riverside Facilities Security Specification v1.2, Section 7.1.1, *Physical Security*, states, 'County facilities are only accessible to authorized individuals with properly coded key cards, authorized keys or access authorization, and access to the premises is by official identification only.' Additionally, National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-12, *An Introduction to Information Security*, Section 10.16, *Personnel Security*, states, 'Organizations ensure that organizational information and systems are protected during and after personnel actions such as terminations or transfers.'

Thirty-nine out of 47 (82%) employees separated from the department did not have badges deactivated timely. Additionally, of the thirty-nine badges not deactivated timely, eighteen (46%) were still active as of the fieldwork date. There are no specific tasks defined in the Information Technology service management system that tracks badge deactivations. Additionally, Information Technology does not have written, formal policies and procedures that guide personnel to deactivate employee badges on the day of separation or transfer from the department. This can lead to unauthorized individuals accessing county facilities and poses a threat to county assets and existing county personnel."

Recommendation 1.1

"Develop procedures to ensure personnel deactivate badges on the day of an employee's separation or transfer from the department and regularly reviews the compliance."

Current Status 1.1: Implemented

Recommendation 1.2

"Ensure the IT service management system task list is updated to include the task specific to badge deactivations."

Current Status 1.2: Implemented

Finding 2: Vulnerability Remediation Tracking

"County of Riverside Information Security Standard v1.0, Section 4.19.5, *Remediation Status,* states, 'Remediation status shall be updated in [the vulnerability management system].'

Remediation progress for unresolved system vulnerabilities need to be tracked and documented to ensure remediation steps available for vulnerabilities do not remain unresolved. We noted four NIST-published, high-risk vulnerabilities during the audit period that were outstanding as of March 1, 2024, with no documented evidence of remediation progress. Remediation progress for the vulnerabilities are not tracked due to limitations in processing large volume of vulnerabilities and the absence of established procedures for monitoring high risk vulnerabilities. The absence of tracking the remediation progress impedes in the ability to closely monitor the implementation status and quickly mitigate any risks posed by the system vulnerabilities."

Recommendation 2

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

Current Status 2: Implemented

Finding 3: Virtual Private Network (VPN) Updates

"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.'

Information Technology's VPN software has not been updated since 2020, while several updates have been made available since then. The department does not have a process in place to track remediation progress for unresolved vulnerabilities, such as using outdated VPN software, and there are potential deployment errors that may affect the county network when updating to the latest VPN version. Outdated VPN software may contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the county network. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences.

On March 19, 2024, Information Technology updated their VPN software to the latest version available that addresses the condition above to improve the adequacy and effectiveness of their internal controls. Specifically, the VPN software update enhances security features and improves functionality. We thank Information Technology for taking a proactive approach to address the condition. In the follow-up audit, we will verify whether the department updates their VPN software timely once new versions become available."

Recommendation 3

"Develop a process to ensure Information Technology's VPN software is updated timely once applicable security related updates to VPN becomes available."

Current Status 3: Implemented

Finding 4: Third-Party Vendor Provisioning

"County of Riverside Information Security Standard v1.0, Section 4.13.1, *Access,* states, 'Individuals not employed by the County wishing to connect to any County system or network shall first execute the Riverside County Information Security 3rd Party Access Agreement and any other applicable agreements.' Additionally, County of Riverside Information Security Standard v1.0, Section 4.14.2, *Expiration,* states, 'Contractor and vendor accounts shall be configured to automatically expire every 15 days, or at the end of the contractor's or vendor's planned visit; whichever comes first.' Lastly, County of Riverside Information Security Standard v1.0, Section 4.15, *Remote Access,* states, 'Remote access for non-county employees shall be reviewed and re-approved on a monthly basis. Two factor authentication is required if the remote client directly connects to an internal network.'

Of the ten vendor VPN accounts randomly selected for testing, we identified the following at the date of fieldwork:

- Four vendor VPN accounts were not duly approved. The department currently utilizes a VPN account form for account approvals. However, there is not a process in place to ensure the forms are completed, signed by department personnel, and stored for retention.

- Seven vendor VPN accounts were inactive over 365 days but were not disabled. Information Technology's Technical Service Bureau (TSB), which controls identity management and Information Technology infrastructure, has a process to disable any accounts that have been inactive for 365 days. However, the script codes being utilized by TSB did not send inactivity alerts to the department, which caused the seven inactive accounts to remain open.

- None of the vendors had two-factor authentication enabled to secure and authenticate the sessions. Information Technology can review which vendors have two-factor authentication enabled. However, the department does not have a process in place to continuously monitor two-factor authentication compliance.

Not approving VPN account forms and reviewing VPN accounts for inactivity, can lead to the creation of invalid, non-active accounts. This creates vulnerabilities that could be exploited by

cyber threat actors, while such risks are enhanced with the absence of two-factor authentication. Not having two-factor authentication increases the risk of unauthorized access, data breaches involving sensitive and confidential information."

Recommendation 4

"Develop a process over allowing third-party vendor VPN accounts to include steps to approve vendor VPN forms, monitor two-factor authentication, and timely disabling of inactive vendor VPN accounts."

Current Status 4: Partially Implemented

Information Technology has made efforts to address the recommendation above by automating the deactivation of accounts that have been inactive for 60 days or more. While this action demonstrates progress, opportunities for improvement remain. Specifically, the department's current processes do not yet support monitoring two-factor authentication for third-party vendors, and the deactivation dates of vendor VPN accounts are not actively monitored or recorded. As a result, accounts could stay active within the 60-day inactivity period even after the vendor no longer requires access.

Management's Response

"We concur that this item is partially implemented. RCIT is researching the implementation of multi-factor authentication (MFA) for vendor accounts. We will collaborate with the Information Security Office and the Auditor to develop a plan for transitioning all vendors to an MFA-supported system.

RCIT implemented a procedure to automatically deactivate vendor accounts that had not logged into the VPN for 60 days. However, it was found that disabling these accounts prevented the vendors from performing other necessary tasks. This is because the same account used for VPN is also used for additional systems that the vendor supports. RCIT will work with departments, the Information Security Office, and the Auditor to find an appropriate solution, as the current process has caused issues for the departments that RCIT supports. RCIT is also in the process of researching additional tools that provide greater visibility into tracking accounts."

Finding 5: Timely Review and Revision of Information Security Standard

"Board of Supervisors Policy A-58, *Information Security Policy,* states, 'Riverside County Chief Information Security Officer (CISO) [is authorized] to develop and maintain the Riverside County

Information Security Program.' This policy requires that the Information Security Standard is maintained to adapt to changing technologies and state and federal regulations.

The County of Riverside Information Security Standard was last revised in 2013 using the third version, or 'Rev 3,' of NIST SP 800-53, *Security and Privacy Control for Information Systems and Organizations.* However, NIST published SP 800-53 "Rev 3" in 2010 and withdrew it in 2014. Since 2014, NIST released 'Rev 4' in 2015 (withdrawn in 2021), and 'Rev 5' is latest applicable.

See Table A below for a summary of NIST SP 800-53 versions:

Table A: NIST SP 800-53 Versions

Description	Version	Published	Withdrawn	Information Technology Standard Timeline
NIST 800-53	Rev1	2006	2008	
NIST 800-53	Rev2	2007	2010	
NIST 800-53	Rev3	2010	2014	2013
NIST 800-53	Rev4	2015	2021	
NIST 800-53	Rev5	2020	To date	2024

Information Technology needs to establish agreed-upon review timeline to ensure the County of Riverside Information Security Standard remains current. Additionally, the department does not have a dedicated compliance team to monitor critical NIST updates that should be reflected in the County of Riverside Information Security Standard. Not reviewing and updating the standards used for network security and controls timely can lead to outdated processes and procedures being utilized by county departments. This compromises county responses to emerging threats and vulnerabilities.

On March 5, 2024, Information Technology finalized the County of Riverside Information Security Standard v2.0 that address the condition above and communicated their efforts to improve the adequacy and effectiveness of their internal controls. Specifically, the updated standards include the most recent and critical NIST updates to enhance access controls and information security processes. We thank Information Technology for taking a proactive approach to address the condition addressed in this finding. In the follow-up audit, we will verify whether the department develops a process to ensure the County of Riverside Information Security Standard includes newly adopted NIST updates and whether a review and revision timeline is included within the document."

Recommendation 5.1

"Develop a process to ensure that the County of Riverside Information Security Standard is updated to reflect the latest NIST changes, while removing policies and procedures that are no longer in practice."

Current Status 5.1: Implemented

Recommendation 5.2

"Develop a process to ensure that the future review and revision timeline is included in the County of Riverside Information Security Standards."

Current Status 5.2: Implemented

Finding 6: Firewall Rules for Operating System Restrictions

"County of Riverside Information Security Standard v1.0, Section 4.13.7, *Internet,* states, 'Rules shall be configured to allow the minimum access required to support county services.' Additionally, 'firewall configurations and rules shall be reviewed by the ISO annually.'

Department firewall rules addressing non-county devices (vendors and foreign devices) do not restrict outdated operating systems. The increasing demand for working remotely requires Information Technology to allow older operating systems for maximum availability for non-county devices, where some county departments do not have resources available for new devices. Allowing outdated operating systems creates security vulnerabilities when using non-county devices. This allows attackers to use a compromised device to move laterally throughout a network by taking advantage of known vulnerabilities, elevated privileges, and potentially hacking once inside."

Recommendation 6

"Develop a process to ensure Information Technology firewall rules allow the minimum access required while restricting and implementing endpoint detection response for outdated operating systems at non-county devices."

Current Status 6: Implemented

Finding 7: ISO Collaboration Over the Final Network Diagram

"County of Riverside Information Security Standard v1.0, Section 4.13, *Networking,* states, 'Final network architecture designs shall require ISO approval prior to implementation.'

Information Technology's final network diagram did not have evidence of Information Security Office review and approval. The department does not have a process in place to formally document Information Security Office approval over the final network diagram. As such, we cannot independently determine whether the Information Security Office reviewed and approved the final network diagram prior to implementation. Not documenting the review and approval of the final network diagram leads to an increased risk of unauthorized changes to the county network without an audit trail of Information Security Office approval for consistency and security validation."

Recommendation 7

"Develop a process to ensure that Information Security Office's review and approval over external facing network diagrams are adequately documented."

Current Status 7: Implemented

Disaster Recovery Plan

Finding 8: Disaster Recovery Plan Formalization

"NIST SP 800-53, Section 3.6, *Contingency Planning*, states, 'The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures.'

Information Technology does not have a written, formal disaster recovery plan. The department has begun to plan for emergencies and county-wide outages. However, there is not a written, formal disaster recovery plan in place that has been approved by senior management. As such, there are no relevant policies, procedures, and communication protocols to independently review and verify. Additionally, the department does not have a process in place to perform comprehensive testing and evaluations of a written, formal disaster recovery plan and alternative processing facilities. The County of Riverside Information Security Standard v1.0 has not been updated to include the requirement of a written, formal disaster recovery plan. Not developing a comprehensive disaster recovery plan may affect system availability upon outages, business continuity, and business resilience.

On March 5, 2024, Information Technology finalized the County of Riverside Information Security Standard v2.0 that laid down the policy for disaster recovery plan. Specifically, the updated standards include the most recent NIST updates for disaster recovery plan. We thank Information Technology for taking a proactive approach to establish policy for disaster recovery plan. In the follow-up audit, we will verify whether the department develops disaster recovery procedures as per the new policy to ensure the County of Riverside Information Technology department has formally documented reviewed and evaluated disaster recovery plan."

Recommendation 8.1

"Develop a written, formal disaster recovery plan and ensure it is formally reviewed and approved by senior management."

Current Status 8.1: Partially Implemented

Information Technology has made progress toward developing a written, formal disaster recovery plan, including establishing a 30-day plan to migrate from the current data center. While these actions represent progress in addressing the audit recommendation above, a complete and comprehensive disaster recovery plan has yet to be finalized.

Management's Response

"We concur that this item is partially implemented. RCIT has started a project to document a written disaster recovery plan, which should be completed within one year (5/1/26)."

Recommendation 8.2

"Develop a process to communicate the disaster recovery plan to appropriate stakeholders."

Current Status 8.2: Partially Implemented

Information Technology is collaborating with the Riverside County Executive Office to standardize which systems require basic recovery and which need more advanced recovery options. Once finalized, the department will communicate the recovery options to appropriate stakeholders.

Management's Response

"We concur that this is partially implemented. The formal disaster recovery plan referenced in recommendation 8.1 will include this information and will be shared with appropriate stakeholders."

Recommendation 8.3

"Develop a process to ensure that the disaster recovery plan is annually tested for the county's critical applications, and an after-action report is developed and reviewed by senior management."

Current Status 8.3: Partially Implemented

Information Technology has made efforts to address the recommendation above by testing the disaster recovery of two critical county applications, with senior management reviewing the related after-action reports. While these actions demonstrate progress, annual testing has not yet been extended to all servers and applications.

Management's Response

"We concur that this is partially implemented. RCIT will work with departments to perform annual testing on a sampling of environments that have disaster recovery protection. A sampling will be used as formal testing will require downtime of the system being tested."

Project Cost Tracking

Finding 9: Internal Project Cost Tracking

"Standard Practice Manual 508, *Intangible Assets – Software*, states, 'Activities involved in developing and installing internally generated computer software and the specifics of each stage can be grouped into the following steps: 1. Preliminary Project Stage: Cost activities should be expensed as incurred… 2. Application Development Stage: Cost activities should be capitalized… 3. Post-Implementation / Operation Stage: Cost activities should be expensed as occurred.' Additionally, Standard Practice Manual 508, *Intangible Assets – Software*, states, 'Capitalize expenditures if modification results in any of the following: 1. An increase in functionality… 2. Increase in efficiency… 3. Extension of estimated useful life.'

Information Technology assigned one project code to three different software modification projects. Additionally, the different phases of the software modification projects were also combined into the same project code. As such, project costs and transactions relating to the different projects and project phases were commingled under one project code. Department personnel overseeing project cost tracking were not provided adequate training or guidance over the applicable Standard Practice Manuals. Not assigning unique project codes to different software modification projects and their respective phases causes difficulties tracking dedicated internal costs related to capitalization, affecting total capitalization costs needed to remain compliant with necessary accounting standards and county policies. Additionally, it leads to inefficiencies when needing to separate costs associated with the development, implementation, and testing phases of a software development or modification project."

Recommendation 9

"Ensure compliance with Standard Practice Manual 508, *Intangible Assets – Software*, by assigning separate project codes for each unique project and phase associated with developing or modifying internally generated computer software. This should emphasize the ability to distinguish between capitalized cost and expenditures by project."

Current Status 9: Implemented

Warranties and Rebates

Finding 10: Warranty Monitoring

"Information Technology's policy titled *RCIT Asset Disposition Notification*, Section 3.3*, Return Merchandise Authorization Procedures*, states, 'When an asset is returned to manufacturer/supplier, a Return Merchandise Authorization (RMA) Notice Form request must be submitted in [the IT service management system] to update Asset status in the inventory records.'

Ten out of sixteen (63%) warranty claims processed during the audit review period remained open after the claims were initially processed. The average days elapsed after claims processing was 260 days, with the longest processed claim remaining open for 427 days and the shortest remaining open for 68 days. The department only assigns warranty-related tasks to capital assets in the IT service management system. As such, tasks over warranty claims for non-capital assets were not finalized and closed for warranty claims in the IT service management system. Leaving the processed warranty claims open obscures the department's list of open claims by commingling processed claims with claims that have yet to be initiated. This causes time-sensitive claims to remain open and potentially miss submission deadlines and adds to the amount of claim resubmissions that could have been avoided."

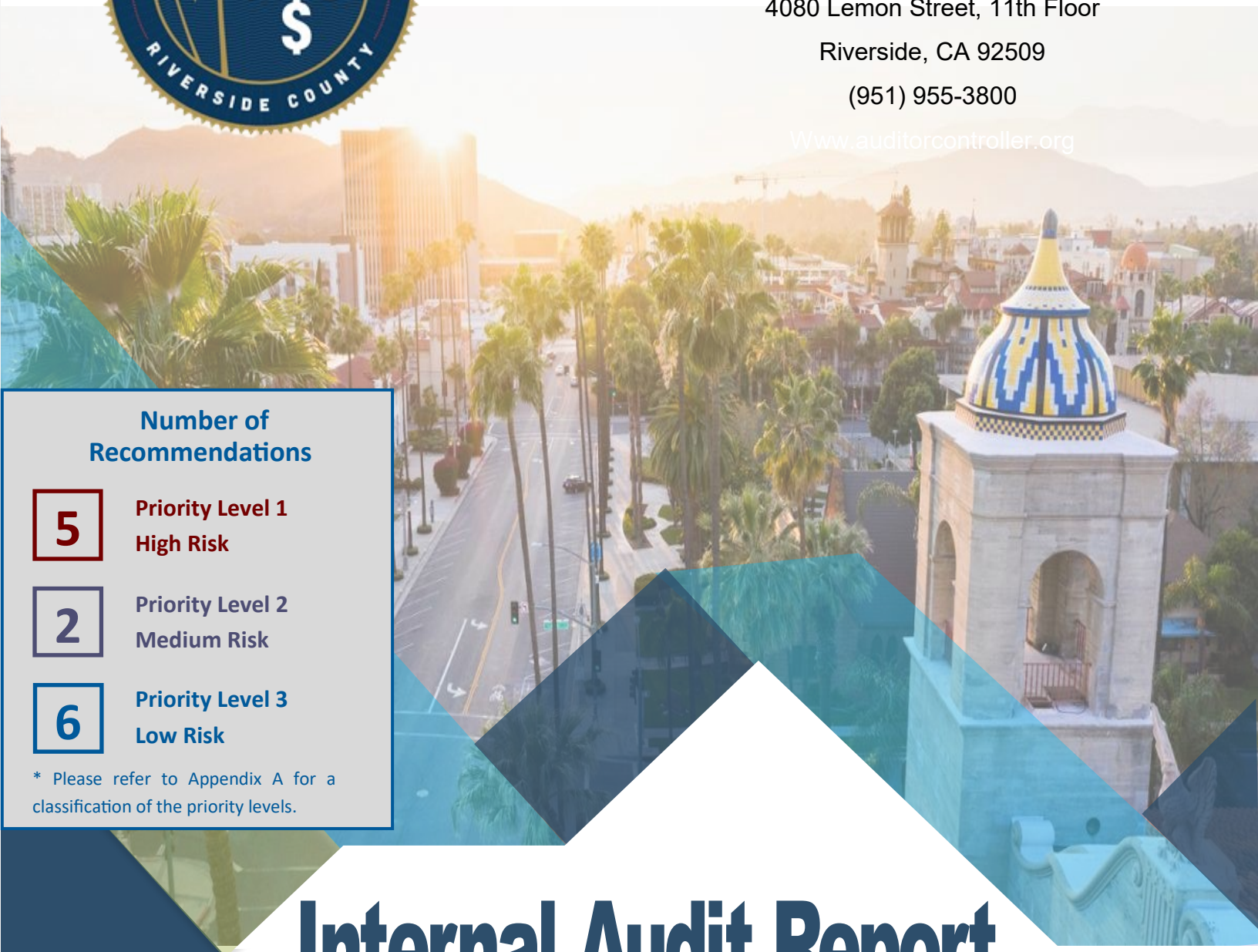
Recommendation 10

"Develop a process to ensure the IT service management system is updated to reflect the actual status of warranty claims."

Current Status 10: Implemented

Attachment A

Office of Ben J. Benoit
Riverside County Auditor-Controller
4080 Lemon Street, 11th Floor
Riverside, CA 92509
(951) 955-3800
Www.auditorcontroller.org



Number of Recommendations

5	**Priority Level 1** High Risk
2	**Priority Level 2** Medium Risk
6	**Priority Level 3** Low Risk

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

Internal Audit Report

2024-009

Riverside County Information Technology Department Audit

June 11, 2024

COUNTY OF RIVERSIDE
OFFICE OF THE AUDITOR-CONTROLLER

Ben J. Benoit, Auditor-Controller
Tanya S. Harris, DPA, CPA, Assistant Auditor-Controller

4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
951-955-3800

June 11, 2024

Jim Smith
Chief Information Officer
Riverside County Information Technology
3450 14th Street
Riverside, CA 92501

Subject: **Internal Audit Report 2024-009: Riverside County Information Technology Audit**

Dear Mr. Smith:

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 access controls, disaster recovery plan, project cost tracking, and warranties and rebates.

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 2024-009: Riverside County Information Technology 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
Dave Rogers, Chief Administrative Officer
Grand Jury

Table of Contents

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, Digital Equity Program, and RivCoPRO. Information Technology fully services 27 separate county departments.

Information Technology has an adopted budget of $103.8 million for FY 2023-24 and 396 adopted positions. *County of Riverside, Fiscal Year 2023-24 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 access controls, disaster recovery plan, project cost tracking, and warranties and rebates. Internal controls are processes designed to provide management reasonable assurance of achieving efficiency of operations, compliance with laws and regulations, and reliability of financial and non-financial information. Reasonable assurance recognizes internal controls have inherent limitations, including cost, mistakes, and intentional efforts to bypass internal controls.

Audit Scope and Methodology

We conducted the audit from October 17, 2023, through January 15, 2024, for operations from July 1, 2021, through November 30, 2023.

AUDIT HIGHLIGHTS

- Separated employee badges need to be deactivated timely.
- Unresolved system vulnerabilities need to be tracked and monitored.
- Updates to the VPN application need to be maintained to the latest version.
- Third-party vendor access into the county network needs to be tracked and monitored.
- Updates and revisions to the Information Security Standard need to be maintained periodically.
- Firewall rules need to be updated to exclude outdated operating systems.

Using a risk-based approach, our scope included the following:

- Access Controls
- Disaster Recovery Plan
- Project Cost Tracking
- Warranties and Rebates

Audit Conclusion

Based on the results of our audit, we have identified improvement opportunities for internal controls over access controls, disaster recovery plan, project cost tracking, and warranties and rebates, that can help ensure department objectives relating to these areas are achieved. Specifically, the improvement opportunities are as follows: Ensure the Information Security Standard, current Virtual Private Network (VPN) application version, and firewall rules are periodically revised and updated; deactivate separated employee badges timely; enhance the monitoring and tracking of network vulnerabilities and third-party access into the county network; ensure the Information Security Office reviews and approves the final network diagram; develop written, formal disaster recovery plan and ensure it is reviewed and approved by senior management; assign unique project IDs to each project cost; and review finalized warranty claims timely.

AUDIT HIGHLIGHTS, CONTINUED

- The final network diagram needs to be formally reviewed and approved by the county Information Security Office.
- A written, formal disaster recovery plan needs to be developed and reviewed and approved by senior management.
- Project costs should be assigned unique project IDs to ensure effective monitoring and tracking.
- Finalized warranty claims need to be reviewed and approved timely.

Access Controls

Background

Information Technology has a security team that monitors the county network for intrusions and employs advanced security tools that block an average of 650,000 cyberattacks daily. Access control management within information systems ensures proper confidentiality, integrity, and availability to the data stored within the system.

The Riverside County Board of Supervisors Policy A-58, *Information Security Policy*, authorizes the county's Chief Information Security Officer (CISO) to establish an Information Security Program and Program Framework that requires all county departments to comply. The CISO manages the Information Security Office (ISO) under the umbrella of the Information Technology.

The Information Security Program consists of the Program Framework, the Information Security Risk Management Methodology, and Information Security Standards. Information Security Risk Management Methodology defines the processes for assessing, accepting, and mitigating information security risk. The Information Security Standards define the specific controls and processes required to mitigate information security risks. These standards are updated as necessary by the Information Security Office.

Objective

To verify the existence and adequacy of internal controls over Information Technology's access controls processes.

Audit Methodology

To accomplish these objectives, we:

- Reviewed the County of Riverside Information Security Standard v1.0.
- Interviewed key personnel and reviewed Information Technology department procedures over access controls.
- Verify whether adequate segregation of duties are in place relating to access controls.
- Obtained a listing of all third-party suppliers utilized by Information Technology who have been granted VPN access to verify approval, password renewal, and two-factor authentication.

- Obtained a listing of all active badges within Information Technology and verified whether the badges were deactivated timely upon employee separation from the department.
- Obtained a listing of Information Technology user IDs during the audit review period and verified access controls over passwords and two-factor authentication.
- Obtained Information Technology's firewall policies and network diagram.
- Reviewed Information Technology's firewall and network diagram for adequate approval and compliance with County of Riverside Information Security Standard v1.0.
- Obtained listings of log sources and verified whether the retention log complies with County of Riverside Information Security Standard v1.0.

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

County of Riverside Facilities Security Specification v1.2, Section 7.1.1, *Physical* Security, states, "County facilities are only accessible to authorized individuals with properly coded key cards, authorized keys or access authorization, and access to the premises is by official identification only." Additionally, National Institute of Standards and Technology's[2] (NIST) Special Publication (SP) 800-12, *An Introduction to Information Security*, Section 10.16, *Personnel Security*, states, "Organizations ensure that organizational information and systems are protected during and after personnel actions such as terminations or transfers."

Thirty-nine out of 47 (82%) employees separated from the department did not have badges deactivated timely. Additionally, of the thirty-nine badges not deactivated timely, eighteen (46%) were still active as of the fieldwork date. There are no specific tasks defined in the Information Technology service management system that tracks badge deactivations. Additionally, Information Technology does not have written, formal policies and procedure that guide personnel to deactivate employee badges on the day of separation or transfer from the department. This can lead to unauthorized individuals accessing county facilities and poses a threat to county assets and existing county personnel.

Recommendation 1.1

Develop procedures to ensure personnel deactivate badges on the day of an employee's separation or transfer from the department and regularly reviews the compliance.

[1] Please see Appendix A (page 24) for a description of the finding priority level classifications.
[2] 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,** Badges for RCIT employees are collected (along with laptops and cell phones) on the employee's last day of service. However, there has not been a process in the offboarding workflow to deactivate the collected badge on the employee's last day of work. This new workflow has been implemented and is currently being tested in ServiceNow for all offboarding going forward. RCIT will review compliance with this new workflow to validate its effectiveness and continue to evaluate the process for any areas of improvement. This proactive approach will help strengthen our security protocols and minimize potential risks associated with badge misuse."

Actual/Estimated Date of Corrective Action: July 1, 2024

Recommendation 1.2

Ensure the IT service management system task list is updated to include the task specific to badge deactivations.

Management's Response:

"Concur, The IT service management system (ServiceNow) has been updated to include tasks specific to badge deactivations. This process is currently being tested and will be implemented shortly. This termination request will soon be accessible to all County Departments, including RCIT. This request triggers a specific task for the Security team to promptly deactivate the badge of the employee when submitted by a Supervisor/Manager. This new offboarding process will allow RCIT to promptly deactivate badges upon an employee's separation or transfer, mitigating the risk of unauthorized access."

Actual/Estimated Date of Corrective Action: July 1, 2024

Finding 2: Vulnerability Remediation Tracking	**Priority Level: 1[3]**

County of Riverside Information Security Standard v1.0, Section 4.19.5, *Remediation Status,* states, "Remediation status shall be updated in [the vulnerability management system]."

Remediation progress for unresolved system vulnerabilities need to be tracked and documented to ensure remediation steps available for vulnerabilities do not remain unresolved. We noted four NIST-published, high-risk vulnerabilities during the audit period that were outstanding as of March 1st, 2024, with no documented evidence of remediation progress. Remediation progress

[3] Please see Appendix A (page 24) for a description of the finding priority level classifications.

for the vulnerabilities are not tracked due to limitations in processing large volume of vulnerabilities and the absence of established procedures for monitoring high risk vulnerabilities. The absence of tracking the remediation progress impedes in the ability to closely monitor the implementation status and quickly mitigate any risks posed by the system vulnerabilities.

Recommendation 2

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

Management's Response:

"**Concur**. Today, our county utilizes over 15,000 different varieties of desktop software, operating systems, and applications. This presents a major challenge in keeping each of them fully patched and always updated. One of the major challenges is that a few departments are running older desktop software and departmental applications that will break if remediated, which could result in an unexpected outage or costly remediation for the department. RCIT will work closer with these departments going forward to identify these systems and work with them on remediation options.

RCIT has also deployed several enterprise security technologies that significantly help mitigate the risks presented by outdated software which include endpoint security, endpoint detection and response (EDR), network detection and response (NDR), attack surface reduction (ASR) rules, DNS security, email security, URL filtering, intrusion prevention system (IPS), and breach and attack simulation (BAS) technologies. Most of these technologies are used to adequately mitigate many security vulnerabilities until RCIT is comfortable that a patch is safe to deploy to thousands of systems, which if deployed prematurely could create a more serious problem than the one we are attempting to remediate.

As new vulnerabilities are discovered and security patches are released daily, RCIT will continue to explore ways to improve its patch management timelines and processes, and vulnerability management processes for identifying, prioritizing, assigning, remediating, and tracking/monitoring outstanding security vulnerabilities and patches."

Actual/Estimated Date of Corrective Action: July 1, 2024

Finding 3: Virtual Private Network (VPN) Updates	**Priority Level: 1[3]**

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."

Information Technology's VPN software has not been updated since 2020, while several updates have been made available since then. The department does not have a process in place to track remediation progress for unresolved vulnerabilities, such as using outdated VPN software, and there are potential deployment errors that may affect the county network when updating to the latest VPN version. Outdated VPN software may contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the county network. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences.

On March 19, 2024, Information Technology updated their VPN software to the latest version available that addresses the condition above to improve the adequacy and effectiveness of their internal controls. Specifically, the VPN software update enhances security features and improves functionality. We thank Information Technology for taking a proactive approach to address the condition. In the follow-up audit, we will verify whether the department updates their VPN software timely once new versions become available.

Recommendation 3

Develop a process to ensure Information Technology's VPN software is updated timely once applicable security related updates to VPN becomes available.

Management's Response:

"**Concur**. RCIT will conduct quarterly reviews of our VPN software, specifically Global Protect, alongside our firewall team and the Information Security Office (ISO). Should critical security vulnerabilities arise that pose a risk to our clients, we will promptly upgrade the Global Protect software. However, not all software upgrades address security issues, or the issues they address are related to systems and scenarios that do not exist in our environment. If we determine that our current version is secure and stable without impacting user productivity, we will exercise discretion in upgrading to the latest version. We will establish a recurring quarterly meeting on the Outlook calendar with no end date to ensure the consistency of these reviews and upgrades."

Actual/Estimated Date of Corrective Action: Completed

Finding 4: Third-Party Vendor Provisioning	**Priority Level: 1[4]**

County of Riverside Information Security Standard v1.0, Section 4.13.1, *Access,* states, "Individuals not employed by the County wishing to connect to any County system or network shall first execute the Riverside County Information Security 3rd Party Access Agreement and any other applicable agreements." Additionally, County of Riverside Information Security Standard

[4] Please see Appendix A (page 24) for a description of the finding priority level classifications.

v1.0, Section 4.14.2, *Expiration,* states, "Contractor and vendor accounts shall be configured to automatically expire every 15 days, or at the end of the contractor's or vendor's planned visit; whichever comes first." Lastly, County of Riverside Information Security Standard v1.0, Section 4.15, *Remote Access,* states, "Remote access for non-county employees shall be reviewed and re-approved on a monthly basis. Two factor authentication is required if the remote client directly connects to an internal network."

Of the ten vendor VPN accounts randomly selected for testing, we identified the following at the date of fieldwork:

- Four vendor VPN accounts were not duly approved. The department currently utilizes a VPN account form for account approvals. However, there is not a process in place to ensure the forms are completed, signed by department personnel, and stored for retention.
- Seven vendor VPN accounts were inactive over 365 days but were not disabled. Information Technology's Technical Service Bureau (TSB), which controls identity management and Information Technology infrastructure, has a process to disable any accounts that have been inactive for 365 days. However, the script codes being utilized by TSB did not send inactivity alerts to the department, which caused the seven inactive accounts to remain open.
- None of the vendors had two-factor authentication enabled to secure and authenticate the sessions. Information Technology can review which vendors have two-factor authentication enabled. However, the department does not have a process in place to continuously monitor two-factor authentication compliance.

Not approving VPN account forms and reviewing VPN accounts for inactivity, can lead to the creation of invalid, non-active accounts. This creates vulnerabilities that could be exploited by cyber threat actors, while such risks are enhanced with the absence of two-factor authentication. Not having two-factor authentication increases the risk of unauthorized access, data breaches involving sensitive and confidential information.

Recommendation 4

Develop a process over allowing third-party vendor VPN accounts to include steps to approve vendor VPN forms, monitor two-factor authentication, and timely disabling of inactive vendor VPN accounts.

Management's Response:

"**Concur**. The current process to create a vendor VPN account through ServiceNow requires the following steps. Steps being taken for improvement will be noted.

- A request from the department to have a vendor VPN account created in ServiceNow. This requires the department to provide vendor information and attach the completed "VPN Access Agreement – Vendor" form that is downloaded from ServiceNow.
    - Improvements being made:
        - Verbiage to be added in ServiceNow to ensure that each request is only for one account and not multiple accounts. This will allow for better auditing of accounts being created.
        - Fields in ServiceNow will be updated to ensure that the information provided is for the Vendor and not the County Staff that is making the request.
- Once submitted, an RCIT operations center employee will review the request and verify all information is complete.
    - Improvements being made:
        - Staff are being trained to verify the accuracy of the "VPN Access Agreement – Vendor" form and not just that the form is completed.
- Additional Process improvements:
    - RCIT will perform audits of VPN creation to verify the process is being followed.
    - RCIT will look at automated process improvements to provide a better mechanism for filling out and storage of VPN request forms.

The process for disabling vendor accounts after 60 days of inactivity was no longer working. RCIT is working to remediate this step and plans to have a process in place that automatically disables accounts after 60 days of inactivity.

RCIT is currently working with Palo Alto on issues that are preventing MFA support for Vendor accounts. MFA for vendor VPN accounts will be prioritized as soon as current issues are resolved."

Actual/Estimated Date of Corrective Action: July 1, 2024 (process improvement, disabling of accounts), and December 21st, 2024 for MFA enforcement of Vendor VPN accounts due to a limitation of the Palo Alto firewall. RCIT is working with Palo Alto to remediate the issue and will update sooner if possible**.**

Finding 5: Timely Review and Revision of Information Security Standard	Priority Level: 2[5]

Board of Supervisors Policy A-58, *Information Security Policy,* states, "Riverside County Chief Information Security Officer (CISO) [is authorized] to develop and maintain the Riverside County

[5] Please see Appendix A (page 24) for a description of the finding priority level classifications.

Information Security Program." This policy requires that the Information Security Standard is maintained to adapt to changing technologies and state and federal regulations.

The County of Riverside Information Security Standard was last revised in 2013 using the third version, or "Rev 3," of NIST SP 800-53, *Security and Privacy Control for Information Systems and Organizations.*[6] However, NIST published SP 800-53 "Rev 3" in 2010 and withdrew it in 2014. Since 2014, NIST released "Rev 4" in 2015 (withdrawn in 2021), and "Rev 5" is latest applicable.

See Table A below for a summary of NIST SP 800-53 versions:

Table A: NIST SP 800-53 Versions

Description	Version	Published	Withdrawn	Information Technology Standard Timeline
NIST 800-53	Rev1	2006	2008	
NIST 800-53	Rev2	2007	2010	
NIST 800-53	Rev3	2010	2014	2013
NIST 800-53	Rev4	2015	2021	
NIST 800-53	Rev5	2020	To date	2024

Information Technology needs to establish agreed-upon review timeline to ensure the County of Riverside Information Security Standard remains current. Additionally, the department does not have a dedicated compliance team to monitor critical NIST updates that should be reflected in the County of Riverside Information Security Standard. Not reviewing and updating the standards used for network security and controls timely can lead to outdated processes and procedures being utilized by county departments. This compromises county responses to emerging threats and vulnerabilities.

On March 5, 2024, Information Technology finalized the County of Riverside Information Security Standard v2.0 that address the condition above and communicated their efforts to improve the adequacy and effectiveness of their internal controls. Specifically, the updated standards include the most recent and critical NIST updates to enhance access controls and information security processes. We thank Information Technology for taking a proactive approach to address the condition addressed in this finding. In the follow-up audit, we will verify whether the department develops a process to ensure the County of Riverside Information Security Standard includes newly adopted NIST updates and whether a review and revision timeline is included within the document.

[6] The Information Security Standard written by Information Technology mirrors the security and application controls documented in the NIST standard and guidelines.

Recommendation 5.1

Develop a process to ensure that the County of Riverside Information Security Standard is updated to reflect the latest NIST changes, while removing policies and procedures that are no longer in practice.

Management's Response:

"Concur. RCIT will develop and implement a process to ensure the information security standard is reviewed and revised on a minimum annual or as-needed basis to maintain alliance with current NIST standards."

Actual/Estimated Date of Corrective Action: July 1, 2024

Recommendation 5.2

Develop a process to ensure that the future review and revision timeline is included in the County of Riverside Information Security Standards.

Management's Response:
"Concur. RCIT will develop and implement a process to ensure all review and revision activities are documented in the Revision History section of the standard."

Actual/Estimated Date of Corrective Action: July 1, 2024

Finding 6: Firewall Rules for Operating System Restrictions	Priority Level: 3[7]

County of Riverside Information Security Standard v1.0, Section 4.13.7, *Internet,* states, **"**Rules shall be configured to allow the minimum access required to support county services." Additionally, "firewall configurations and rules shall be reviewed by the ISO annually."

Department firewall rules addressing non-county devices (vendors and foreign devices) do not restrict outdated operating systems. The increasing demand for working remotely requires Information Technology to allow older operating systems for maximum availability for non-county devices, where some county departments do not have resources available for new devices. Allowing outdated operating systems creates security vulnerabilities when using non-county devices. This allows attackers to use a compromised device to move laterally throughout a network by taking advantage of known vulnerabilities, elevated privileges, and potentially hacking once inside.

[7] Please see Appendix A (page 24) for a description of the finding priority level classifications.

Recommendation 6

Develop a process to ensure Information Technology firewall rules allow the minimum access required while restricting and implementing endpoint detection response for outdated operating systems at non-county devices.

Management's Response:

"Concur. RCIT will leverage the host information profile (HIP) feature on its enterprise firewalls to ensure all endpoints connecting to the county network over VPN have the latest security patches installed, an antivirus program installed, and a supported operating system installed before granting access to the county network."

Actual/Estimated Date of Corrective Action: July 1, 2024

Finding 7: ISO Collaboration Over the Final Network Diagram	Priority Level: 3[8]

County of Riverside Information Security Standard v1.0, Section 4.13, *Networking,* states, "Final network architecture designs shall require ISO approval prior to implementation."

Information Technology's final network diagram did not have evidence of Information Security Office review and approval. The department does not have a process in place to formally document Information Security Office approval over the final network diagram. As such, we cannot independently determine whether the Information Security Office reviewed and approved the final network diagram prior to implementation. Not documenting the review and approval of the final network diagram leads to an increased risk of unauthorized changes to the county network without an audit trail of Information Security Office approval for consistency and security validation.

Recommendation 7

Develop a process to ensure that Information Security Office's review and approval over external facing network diagrams are adequately documented.

Management's Response:
"Concur. RCIT will implement a structured process in collaboration with the ISO to solicit review and approval for all Public Facing Network diagrams. While ISO approval will be required for diagrams on external-facing networks, those exclusively internal to CORNET and contained within the firewall perimeter will not necessitate ISO endorsement. This approach ensures that

[8] Please see Appendix A (page 24) for a description of the finding priority level classifications.

our external network architecture receives the appropriate scrutiny and validation while maintaining efficiency for internal network documentation."

Actual/Estimated Date of Corrective Action: Complete

Disaster Recovery Plan

Background

One of Information Technology's main objectives is to provide a secure technology infrastructure to protect county data and minimize risk. Information Technology's disaster recovery plan over critical applications is planned to be cloud-based. If a system application goes down, the cloud-based solution allows Information Technology's critical applications to restore within a reasonable amount of time. The department implemented phase one of their disaster recovery plan, in which one critical application has been synced to their cloud-based server to prevent extensive downtime in the event of a system-wide outage. Information Technology is planning to identify additional applications to be included in their disaster recovery plan for the second phase. The department added redundancy in authentication, power, and networking as well. Also, formal training for unplanned downtime is given to Information Technology personnel.

Objective

To verify the existence and adequacy of internal controls over Information Technology's disaster recovery plan.

Audit Methodology

To accomplish these objectives, we:

- Reviewed County of Riverside Information Security Standard v1.0.
- Interviewed key personnel and reviewed department procedures over their disaster recovery plan.
- Reviewed Information Technology's disaster recovery plan and benchmarked with requirements from NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.

Finding 8: Disaster Recovery Plan Formalization	Priority Level: 3[9]

NIST SP 800-53, Section 3.6, *Contingency Planning*, states, "The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures."

Information Technology does not have a written, formal disaster recovery plan. The department has begun to plan for emergencies and county-wide outages. However, there is not a written, formal disaster recovery plan in place that has been approved by senior management. As such, there are no relevant policies, procedures, and communication protocols to independently review and verify. Additionally, the department does not have a process in place to perform comprehensive testing and evaluations of a written, formal disaster recovery plan and alternative processing facilities. The County of Riverside Information Security Standard v1.0 has not been updated to include the requirement of a written, formal disaster recovery plan. Not developing a comprehensive disaster recovery plan may affect system availability upon outages, business continuity, and business resilience.

On March 5, 2024, Information Technology finalized the County of Riverside Information Security Standard v2.0 that laid down the policy for disaster recovery plan. Specifically, the updated standards include the most recent NIST updates for disaster recovery plan. We thank Information Technology for taking a proactive approach to establish policy for disaster recovery plan. In the follow-up audit, we will verify whether the department develops disaster recovery procedures as per the new policy to ensure the County of Riverside Information Technology department has formally documented reviewed and evaluated disaster recovery plan.

Recommendation 8.1

Develop a written, formal disaster recovery plan and ensure it is formally reviewed and approved by senior management.

Management's Response:
"Concur. RCIT is in the process of creating a formal documented Disaster Recovery Plan and plans to have the first iteration of the document completed in 6 to 9 months.
Although not formally documented, RCIT did have components of a disaster recovery plan in place prior to the audit performed by the Auditor-Controller. These items include the following:

- Backups for 60 days (there is a current project in place to increase backup availability to 365 days).

[9] Please see Appendix A (page 24) for a description of the finding priority level classifications.

- A cloud-based disaster recovery environment that is available on demand and hyper-scalable (there are current projects in place to increase our resiliency by preparing additional cloud environments/vendors that can be leveraged in "DR" scenarios).
- Dedicated network connections to current cloud environments (there are projects in place to create dedicated network connections to the additional cloud environments/vendors)."

Actual/Estimated Date of Corrective Action: March 1, 2025

Recommendation 8.2

Develop a process to communicate the disaster recovery plan to appropriate stakeholders.

Management's Response:
"Concur. The process of communicating the disaster recovery plan will be incorporated into the formal disaster recovery plan mentioned in recommendation 8.1."

Actual/Estimated Date of Corrective Action: March 1, 2025

Recommendation 8.3

Develop a process to ensure that the disaster recovery plan is annually tested for the county's critical applications, and an after-action report is developed and reviewed by senior management.

Management's Response:
"Concur. The disaster recovery testing process will be incorporated into the formal disaster recovery plan mentioned in recommendation 8.1. RCIT manages several hundred systems and testing each of them annually would be extremely time-consuming and unpractical. RCIT will work with the Executive Office to identify the most critical systems and develop detailed plans to recover them in the event of a disaster. A general recovery plan will be developed for the remaining systems, many of which may require third-party vendor support."

Actual/Estimated Date of Corrective Action: March 1, 2025

Project Cost Tracking

Background

Information Technology provides a variety of services to county departments, including applications development, operations support services, help desk services, field support, data center server and storage services, project management, and additional support services.

Construction-in-progress (CIP) is an account used to record capitalized costs related to assets that are not yet substantially ready to be placed in service. CIP is used to record the costs of direct labor, direct material, and overhead amounts that are expended in one fiscal year on new construction, land or building improvements, or other tangible and intangible capital construction projects that will be finished in a future year. CIP projects related to building and infrastructure with an estimated project cost greater than $5,000 must be capitalized. Upon completion of the projects, the related costs that have accumulated in the CIP accounts will begin to depreciate based on the estimated useful life of the newly completed capital asset.

Objective

To verify the existence and adequacy of internal controls over Information Technology's project cost tracking process.

Audit Methodology

- Obtained an understanding of department processes and procedures over project cost tracking.
- Interviewed key personnel regarding the departments project cost tracking process.
- Obtained a listing of all active, inactive, and overdue CIP projects during the audit review period and selected a random sample for review.
- Examined supporting documentation related to the selected CIP projects.
- Reviewed the minute orders for project details and for the scope of work.
- Reviewed expenditure reconciliations over the selected CIP projects.
- Verified whether the selected CIP projects were in compliance with appropriate Standard Practice Manuals and Governmental Accounting Standard Board Statements.
- Verified whether selected CIP projects were regularly compared with budgeted or estimated costs.

Finding 9: Internal Project Cost Tracking	Priority Level: 3[10]

Standard Practice Manual 508, *Intangible Assets – Software*, states, "Activities involved in developing and installing internally generated computer software and the specifics of each stage can be grouped into the following steps: 1. Preliminary Project Stage: Cost activities should be expensed as incurred… 2. Application Development Stage: Cost activities should be capitalized… 3. Post-Implementation / Operation Stage: Cost activities should be expensed as occurred." Additionally, Standard Practice Manual 508, *Intangible Assets – Software*, states, "Capitalize expenditures if modification results in any of the following: 1. An increase in functionality… 2. Increase in efficiency… 3. Extension of estimated useful life."

Information Technology assigned one project code to three different software modification projects. Additionally, the different phases of the software modification projects were also combined into the same project code. As such, project costs and transactions relating to the different projects and project phases were commingled under one project code. Department personnel overseeing project cost tracking were not provided adequate training or guidance over the applicable Standard Practice Manuals. Not assigning unique project codes to different software modification projects and their respective phases causes difficulties tracking dedicated internal costs related to capitalization, affecting total capitalization costs needed to remain compliant with necessary accounting standards and county policies. Additionally, it leads to inefficiencies when needing to separate costs associated with the development, implementation, and testing phases of a software development or modification project.

Recommendation 9

Ensure compliance with Standard Practice Manual 508, *Intangible Assets – Software*, by assigning separate project codes for each unique project and phase associated with developing or modifying internally generated computer software. This should emphasize the ability to distinguish between capitalized cost and expenditures by project.

Management's Response:

"Concur. RCIT understands the importance of ensuring compliance with County Standards. In the future, when a CIP project has been identified (and there have been only two in over 10 years), RCIT fiscal will work with the project managers to ensure phases of the project are clearly identified and assign a program/activity code. We realize the importance of ensuring compliance with county standard codes to separate those costs into appropriate categories. RCIT has reached out to the Auditor's General Accounting unit for guidance regarding the Standard."

Actual/Estimated Date of Corrective Action: Completed

[10] Please see Appendix A (page 24) for a description of the finding priority level classifications.

Warranties and Rebates

Background

Warranties and rebates are integral components of departmental transactions that serve to provide assurances and incentives to both consumers and suppliers. Warranties build confidence in consumers by promising remedies or replacements in the event of product defects of failures within a specified period. Rebates are financial incentives offered by suppliers to customers as a form of discount or refund after the purchase of goods or services. Utilizing both warranties and rebates are methods county departments may use to reduce the cost of conducting business and saving taxpayer dollars. Some of Information Technology's assets, such as computers, network equipment, and various other electronics, are eligible to participate in warranty and rebate programs. Warranties and rebates are monitored by Information Technology's Procurement Management Group working under the Facilities and Administration division. This involves establishing guidelines for eligible warranty and rebate terms, accompanied by retaining supporting documentation for each transaction.

Objective

To verify the existence and adequacy of internal controls over Information Technology's warranties and rebates process.

Audit Methodology

- Obtained an understanding of department processes and procedures over monitoring and tracking warranties and rebates.
- Conducted interviews with department management and personnel over warranties and rebates.
- Obtained a listing of all rebates obtained and captured during the audit review period.
- Obtained a listing of all equipment failures and replacements during the audit review period.
- Obtained a report detailing all department assets and their associated warranties.
- Obtained a listing of all capital and non-capital asset disposals during the audit review period.
- Verified whether the warranty claims were appropriate, supporting documentation was adequate, and the transactions were reviewed and approved.
- Verified whether rebates were processed timely.

Finding 10: Warranty Monitoring	Priority Level: 3[11]

Information Technology's policy titled *RCIT Asset Disposition Notification*, Section 3.3*, Return Merchandise Authorization Procedures*, states, "When an asset is returned to manufacturer/supplier, a Return Merchandise Authorization (RMA) Notice Form request must be submitted in [the IT service management system] to update Asset status in the inventory records."

Ten out of sixteen (63%) warranty claims processed during the audit review period remained open after the claims were initially processed. The average days elapsed after claims processing was 260 days, with the longest processed claim remaining open for 427 days and the shortest remaining open for 68 days. The department only assigns warranty-related tasks to capital assets in the IT service management system. As such, tasks over warranty claims for non-capital assets were not finalized and closed for warranty claims in the IT service management system. Leaving the processed warranty claims open obscures the department's list of open claims by commingling processed claims with claims that have yet to be initiated. This causes time-sensitive claims to remain open and potentially miss submission deadlines and adds to the amount of claim resubmissions that could have been avoided.

Recommendation 10

Develop a process to ensure the IT service management system is updated to reflect the actual status of warranty claims.

Management's Response:
"Concur. When a warranty claim is submitted in the IT service management system, a task is deployed to two separate teams, the Warehouse team and the Asset team. The Warehouse team works with the vendor and the bureau to ensure the warranty claim is completed. All sixteen warranty claims were completed and closed by the Warehouse team. The Asset team also receives a task to which they confirm whether the item is a capital asset. The ten warranty claims that remained open were not closed by the Asset team because these items were not trackable assets. However, staff have now been instructed to close the task with a note referencing 'non-asset'."

Actual/Estimated Date of Corrective Action: Completed

[11] Please see Appendix A (page 24) for a description of the finding priority level classifications.

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

JIM SMITH
Chief Information Officer

DARRYL POLK
Chief Technology Officer

TRACY TILLMAN
Deputy Director Admin – IT

ANTHONY CHOGYOJI
Chief Information Security Officer

MARTIN PEREZ, ACIO
Enterprise Applications Bureau

GUSTAVO VAZQUEZ, ACIO
Converged Communications Bureau

KARAN CHANDRAN, ACIO
Technology Services Bureau

February 24, 2025

Rene Casillas
Deputy Auditor-Controller, Auditor
Riverside County Auditor-Controller Office
4080 Lemon Street, 6th Floor
Riverside, CA 92502

Subject: Internal Audit Report 2025-312: Riverside County Information Technology Follow-up Audit- Department Response

Dear Mr. Casillas:

The following are the current status of the reported findings and planned corrective actions contained in Internal Audit Report 2024-009: Riverside County Information Technology Audit.

Jim Smith — 2-24-2025

Authorized Signature **Date**

Finding 1: Termination of Badge Access

"County of Riverside Facilities Security Specification v1.2, Section 7.1.1, *Physical Security*, states, 'County facilities are only accessible to authorized individuals with properly coded key cards, authorized keys or access authorization, and access to the premises is by official identification only.' Additionally, National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-12, *An Introduction to Information Security*, Section 10.16, *Personnel Security*, states, 'Organizations ensure that organizational information and systems are protected during and after personnel actions such as terminations or transfers.'

Thirty-nine out of 47 (82%) employees separated from the department did not have badges deactivated timely. Additionally, of the thirty-nine badges not deactivated timely, eighteen (46%) were still active as of the fieldwork date. There are no specific tasks defined in the Information Technology service management system that tracks badge deactivations. Additionally,

Information Technology does not have written, formal policies and procedure that guide personnel to deactivate employee badges on the day of separation or transfer from the department. This can lead to unauthorized individuals accessing county facilities and poses a threat to county assets and existing county personnel."

Current Status

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

Recommendation 1.1

"Develop procedures to ensure personnel deactivate badges on the day of an employee's separation or transfer from the department and regularly reviews the compliance."

Management Reply

"**Concur**. Badges for RCIT employees are collected (along with laptops and cell phones) on the employee's last day of service. However, there has not been a process in the offboarding workflow to deactivate the collected badge on the employee's last day of work. This new workflow has been implemented and is currently being tested in ServiceNow for all offboarding going forward. RCIT will review compliance with this new workflow to validate its effectiveness and continue to evaluate the process for any areas of improvement. This proactive approach will help strengthen our security protocols and minimize potential risks associated with badge misuse."

Actual/Estimated Date of Corrective Action: July 1, 2024

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).

Last year, we successfully tested and fully implemented a standardized workflow for offboarding employees within ServiceNow, aimed at ensuring a structured and efficient badge deactivation process. When an RCIT Supervisor has an employee leaving the department, they submit a ServiceNow request, which automatically generates a task (ticket) assigned to the Security Team. This task specifies the required date and time for badge deactivation. This standardized workflow has been operational since October 2024. In urgent situations requiring immediate badge deactivation, a direct call can be made to the Security Team. In such cases, the staff member receiving the request promptly creates a corresponding ServiceNow ticket to document the action and ensure proper tracking.

Recommendation 1.2

"Ensure the IT service management system task list is updated to include the task specific to badge deactivations."

Management Reply

"**Concur**. The IT service management system (ServiceNow) has been updated to include tasks specific to badge deactivations. This process is currently being tested and will be implemented shortly. This termination request will soon be accessible to all County Departments, including RCIT. This request triggers a specific task for the Security team to promptly deactivate the badge of the employee when submitted by a Supervisor/Manager. This new offboarding process will allow RCIT to promptly deactivate badges upon an employee's separation or transfer, mitigating the risk of unauthorized access."

Actual/Estimated Date of Corrective Action: July 1, 2024

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).

Refer to 1.1

Finding 2: Vulnerability Remediation Tracking

"County of Riverside Information Security Standard v1.0, Section 4.19.5, *Remediation Status*, states, 'Remediation status shall be updated in [the vulnerability management system].'

Remediation progress for unresolved system vulnerabilities need to be tracked and documented to ensure remediation steps available for vulnerabilities do not remain unresolved. We noted four NIST-published, high-risk vulnerabilities during the audit period that were outstanding as of March 1st, 2024, with no documented evidence of remediation progress. Remediation progress for the vulnerabilities are not tracked due to limitations in processing large volume of vulnerabilities and the absence of established procedures for monitoring high risk vulnerabilities. The absence of tracking the remediation progress impedes in the 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 2

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

Management Reply

"**Concur**. Today, our county utilizes over 15,000 different varieties of desktop software, operating systems, and applications. This presents a major challenge in keeping each of them fully patched and always updated. One of the major challenges is that a few departments are running older desktop software and departmental applications that will break if remediated, which could result in an unexpected outage or costly remediation for the department. RCIT will work closer with these departments going forward to identify these systems and work with them on remediation options.

RCIT has also deployed several enterprise security technologies that significantly help mitigate the risks presented by outdated software which include endpoint security, endpoint detection and response (EDR), network detection and response (NDR), attack surface reduction (ASR) rules, DNS security, email security, URL filtering, intrusion prevention system (IPS), and breach and attack simulation (BAS) technologies. Most of these technologies are used to adequately mitigate many security vulnerabilities until RCIT is comfortable that a patch is safe to deploy to thousands of systems, which if deployed prematurely could create a more serious problem than the one we are attempting to remediate.

As new vulnerabilities are discovered and security patches are released daily, RCIT will continue to explore ways to improve its patch management timelines and processes, and vulnerability management processes for identifying, prioritizing, assigning, remediating, and tracking/monitoring outstanding security vulnerabilities and patches."

Actual/Estimated Date of Corrective Action: July 1, 2024

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).

RCIT's Technical Services Bureau (TSB) is now utilizing a combination of Microsoft System Center Configuration Manager (SCCM), Microsoft Windows Update for Business, Microsoft Azure Update Manager, and SolarWinds Patch Manager to manage (deploy and track) software updates and security patches for Microsoft operating systems and applications, as well as third-party software (e.g., Adobe, Zoom), while RCIT's Information Security Office (ISO) utilizes Rapid7 Nexpose to scan and report on all software vulnerabilities for all devices connected to the county network. All outstanding vulnerabilities will be documented, tracked, assigned to the appropriate support teams, monitored, and escalated as needed, in ServiceNow.

Finding 3: Virtual Private Network (VPN) Updates

"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.'

Information Technology's VPN software has not been updated since 2020, while several updates have been made available since then. The department does not have a process in place to track remediation progress for unresolved vulnerabilities, such as using outdated VPN software, and there are potential deployment errors that may affect the county network when updating to the latest VPN version. Outdated VPN software may contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the county network. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences.

On March 19, 2024, Information Technology updated their VPN software to the latest version available that addresses the condition above to improve the adequacy and effectiveness of their internal controls. Specifically, the VPN software update enhances security features and improves functionality. We thank Information Technology for taking a proactive approach to address the condition. In the follow-up audit, we will verify whether the department updates their VPN software timely once new versions become available."

Current Status

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

Recommendation 3

"Develop a process to ensure Information Technology's VPN software is updated timely once applicable security related updates to VPN becomes available."

Management Reply

"**Concur**. RCIT will conduct quarterly reviews of our VPN software, specifically Global Protect, alongside our firewall team and the Information Security Office (ISO). Should critical security vulnerabilities arise that pose a risk to our clients, we will promptly upgrade the Global Protect software. However, not all software upgrades address security issues, or the issues they address are related to systems and scenarios that do not exist in our environment. If we determine that our current version is secure and stable without impacting user productivity, we will exercise discretion in upgrading to the latest version. We will establish a recurring quarterly meeting on the Outlook calendar with no end date to ensure the consistency of these reviews and upgrades."

Actual/Estimated Date of Corrective Action: Completed

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).

Since October 2024, RCIT has implemented quarterly meetings between our Converged Communication Bureau (CCB) and Information Security Office (ISO) to review our VPN software (Global Protect) as well as the current and latest firewall PANOS. We are currently running GP Client 6.2.6 and PANOS 11.1.5-h1.

Finding 4: Third-Party Vendor Provisioning

"County of Riverside Information Security Standard v1.0, Section 4.13.1, *Access*, states, 'Individuals not employed by the County wishing to connect to any County system or network shall first execute the Riverside County Information Security 3rd Party Access Agreement and any other applicable agreements.' Additionally, County of Riverside Information Security Standard v1.0, Section 4.14.2, *Expiration*, states, 'Contractor and vendor accounts shall be configured to automatically expire every 15 days, or at the end of the contractor's or vendor's planned visit; whichever comes first.' Lastly, County of Riverside Information Security Standard v1.0, Section 4.15, *Remote Access*, states, 'Remote access for non-county employees shall be reviewed and re-approved on a monthly basis. Two factor authentication is required if the remote client directly connects to an internal network.'

Of the ten vendor VPN accounts randomly selected for testing, we identified the following at the date of fieldwork:

- Four vendor VPN accounts were not duly approved. The department currently utilizes a VPN account form for account approvals. However, there is not a process in place to ensure the forms are completed, signed by department personnel, and stored for retention.
- Seven vendor VPN accounts were inactive over 365 days but were not disabled. Information Technology's Technical Service Bureau (TSB), which controls identity management and Information Technology infrastructure, has a process to disable any accounts that have been inactive for 365 days. However, the script codes being utilized by TSB did not send inactivity alerts to the department, which caused the seven inactive accounts to remain open.
- None of the vendors had two-factor authentication enabled to secure and authenticate the sessions. Information Technology can review which vendors have two-factor authentication enabled. However, the department does not have a process in place to continuously monitor two-factor authentication compliance.

Not approving VPN account forms and reviewing VPN accounts for inactivity, can lead to the creation of invalid, non-active accounts. This creates vulnerabilities that could be exploited by cyber threat actors, while such risks are enhanced with the absence of two-factor authentication. Not having two-factor authentication increases the risk of unauthorized access, data breaches involving sensitive and confidential information."

Current Status

Reported Finding Corrected? ☐ **Yes** ☐ **No**

Partially Implemented

Recommendation 4

"Develop a process over allowing third-party vendor VPN accounts to include steps to approve vendor VPN forms, monitor two-factor authentication, and timely disabling of inactive vendor VPN accounts."

Management Reply

"**Concur**. The current process to create a vendor VPN account through ServiceNow requires the following steps. Steps being taken for improvement will be noted.

- A request from the department to have a vendor VPN account created in ServiceNow. This requires the department to provide vendor information and attach the completed 'VPN Access Agreement – Vendor' form that is downloaded from ServiceNow.
    - Improvements being made:

        - Verbiage to be added in ServiceNow to ensure that each request is only for one account and not multiple accounts. This will allow for better auditing of accounts being created.
        - Fields in ServiceNow will be updated to ensure that the information provided is for the Vendor and not the County Staff that is making the request.
- Once submitted, an RCIT operations center employee will review the request and verify all information is complete.
    - Improvements being made:
        - Staff are being trained to verify the accuracy of the 'VPN Access Agreement – Vendor' form and not just that the form is completed.
- Additional Process improvements:
    - RCIT will perform audits of VPN creation to verify the process is being followed.
    - RCIT will look at automated process improvements to provide a better mechanism for filling out and storage of VPN request forms.

The process for disabling vendor accounts after 60 days of inactivity was no longer working. RCIT is working to remediate this step and plans to have a process in place that automatically disables accounts after 60 days of inactivity.

RCIT is currently working with Palo Alto on issues that are preventing MFA support for Vendor accounts. MFA for vendor VPN accounts will be prioritized as soon as current issues are resolved."

Actual/Estimated Date of Corrective Action: July 1, 2024 (process improvement, disabling of accounts), and December 21st, 2024 for MFA enforcement of Vendor VPN accounts due to a limitation of the Palo Alto firewall. RCIT is working with Palo Alto to remediate the issue and will update sooner if possible.

Current Status

Corrective Action: ☐ **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 do have a process for allowing third-party vendor VPN accounts, which includes approval steps. We have also implemented a process to disable all vendor VPN accounts that have been inactive for over 60 days. We currently do not have two-factor authentication for VPN for Vendors but will work with CCB and devise a solution to implement it. The solution may require funding and, in that case, will be contingent on getting the funding.

Finding 5: Timely Review and Revision of Information Security Standard

"Board of Supervisors Policy A-58, *Information Security Policy,* states, 'Riverside County Chief Information Security Officer (CISO) [is authorized] to develop and maintain the Riverside County

Information Security Program.' This policy requires that the Information Security Standard is maintained to adapt to changing technologies and state and federal regulations.

The County of Riverside Information Security Standard was last revised in 2013 using the third version, or 'Rev 3,' of NIST SP 800-53, *Security and Privacy Control for Information Systems and Organizations.* However, NIST published SP 800-53 'Rev 3' in 2010 and withdrew it in 2014. Since 2014, NIST released 'Rev 4' in 2015 (withdrawn in 2021), and 'Rev 5' is latest applicable.

See Table A below for a summary of NIST SP 800-53 versions:

Table A: NIST SP 800-53 Versions

Description	Version	Published	Withdrawn	Information Technology Standard Timeline
NIST 800-53	Rev1	2006	2008	
NIST 800-53	Rev2	2007	2010	
NIST 800-53	Rev3	2010	2014	2013
NIST 800-53	Rev4	2015	2021	
NIST 800-53	Rev5	2020	To date	2024

Information Technology needs to establish agreed-upon review timeline to ensure the County of Riverside Information Security Standard remains current. Additionally, the department does not have a dedicated compliance team to monitor critical NIST updates that should be reflected in the County of Riverside Information Security Standard. Not reviewing and updating the standards used for network security and controls timely can lead to outdated processes and procedures being utilized by county departments. This compromises county responses to emerging threats and vulnerabilities.

On March 5, 2024, Information Technology finalized the County of Riverside Information Security Standard v2.0 that address the condition above and communicated their efforts to improve the adequacy and effectiveness of their internal controls. Specifically, the updated standards include the most recent and critical NIST updates to enhance access controls and information security processes. We thank Information Technology for taking a proactive approach to address the condition addressed in this finding. In the follow-up audit, we will verify whether the department develops a process to ensure the County of Riverside Information Security Standard includes newly adopted NIST updates and whether a review and revision timeline is included within the document."

Current Status

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

Recommendation 5.1

"Develop a process to ensure that the County of Riverside Information Security Standard is updated to reflect the latest NIST changes, while removing policies and procedures that are no longer in practice."

Management Reply

"**Concur**. RCIT will develop and implement a process to ensure the information security standard is reviewed and revised on a minimum annual or as-needed basis to maintain alliance with current NIST standards."

Actual/Estimated Date of Corrective Action: July 1, 2024

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).

RCIT has developed and implemented a formal procedure to review and update the county's Information Security Standard on a minimum annual or as-needed basis. The last formal review was completed in October 2024 and found that the Standard was in alignment with the latest NIST Cybersecurity Framework (CSF). RCIT's Information Security Office also subscribes to NIST alerts to stay informed of new CSF updates as soon as they become available/published.

Recommendation 5.2

"Develop a process to ensure that the future review and revision timeline is included in the County of Riverside Information Security Standards."

Management Reply

"**Concur**. RCIT will develop and implement a process to ensure all review and revision activities are documented in the Revision History section of the standard."

Actual/Estimated Date of Corrective Action: July 1, 2024

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 county's latest Information Security Standard (Version 2.0) includes a revision history table that now reflects all formal review and revision activities that have been completed.

Finding 6: Firewall Rules for Operating System Restrictions

"County of Riverside Information Security Standard v1.0, Section 4.13.7, *Internet,* states, 'Rules shall be configured to allow the minimum access required to support county services.' Additionally, 'firewall configurations and rules shall be reviewed by the ISO annually.'

Department firewall rules addressing non-county devices (vendors and foreign devices) do not restrict outdated operating systems. The increasing demand for working remotely requires Information Technology to allow older operating systems for maximum availability for non-county devices, where some county departments do not have resources available for new devices. Allowing outdated operating systems creates security vulnerabilities when using non-county devices. This allows attackers to use a compromised device to move laterally throughout a network by taking advantage of known vulnerabilities, elevated privileges, and potentially hacking once inside."

Current Status

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

Recommendation 6

"Develop a process to ensure Information Technology firewall rules allow the minimum access required while restricting and implementing endpoint detection response for outdated operating systems at non-county devices."

Management Reply

"**Concur**. RCIT will leverage the host information profile (HIP) feature on its enterprise firewalls to ensure all endpoints connecting to the county network over VPN have the latest security patches installed, an antivirus program installed, and a supported operating system installed before granting access to the county network."

Actual/Estimated Date of Corrective Action: July 1, 2024

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).

RCIT has successfully implemented and is actively enforcing the host information profile (HIP) feature in the county's enterprise firewall VPN client software to restrict devices running outdated/non-supported operating systems from connecting to the county's network.

Finding 7: ISO Collaboration Over the Final Network Diagram

"County of Riverside Information Security Standard v1.0, Section 4.13, *Networking,* states, 'Final network architecture designs shall require ISO approval prior to implementation.'

Information Technology's final network diagram did not have evidence of Information Security Office review and approval. The department does not have a process in place to formally document Information Security Office approval over the final network diagram. As such, we cannot independently determine whether the Information Security Office reviewed and approved the final network diagram prior to implementation. Not documenting the review and approval of the final network diagram leads to an increased risk of unauthorized changes to the county network without an audit trail of Information Security Office approval for consistency and security validation."

Current Status

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

Recommendation 7

"Develop a process to ensure that Information Security Office's review and approval over external facing network diagrams are adequately documented."

Management Reply

"**Concur**. RCIT will implement a structured process in collaboration with the ISO to solicit review and approval for all Public Facing Network diagrams. While ISO approval will be required for diagrams on external-facing networks, those exclusively internal to CORNET and contained within the firewall perimeter will not necessitate ISO endorsement. This approach ensures that our

external network architecture receives the appropriate scrutiny and validation while maintaining efficiency for internal network documentation."

Actual/Estimated Date of Corrective Action: Complete

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).

RCIT's Converged Communications Bureau (CCB) and Information Security Office (ISO) have been actively engaged and collaborating on the county's new enterprise network architecture and design which will offer greater resiliency through Multiprotocol Label Switching (MPLS) and increased performance and security through upgraded network perimeter firewalls and faster internet circuits. The new network architecture diagram dated 8/19/24 has been reviewed and approved by the ISO and any requested firewall rule changes (add, remove, and modify) are formally reviewed and approved/rejected by the ISO and are tracked in ServiceNow.

Finding 8: Disaster Recovery Plan Formalization

"NIST SP 800-53, Section 3.6, *Contingency Planning*, states, 'The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures.'

Information Technology does not have a written, formal disaster recovery plan. The department has begun to plan for emergencies and county-wide outages. However, there is not a written, formal disaster recovery plan in place that has been approved by senior management. As such, there are no relevant policies, procedures, and communication protocols to independently review and verify. Additionally, the department does not have a process in place to perform comprehensive testing and evaluations of a written, formal disaster recovery plan and alternative processing facilities. The County of Riverside Information Security Standard v1.0 has not been updated to include the requirement of a written, formal disaster recovery plan. Not developing a comprehensive disaster recovery plan may affect system availability upon outages, business continuity, and business resilience.

On March 5, 2024, Information Technology finalized the County of Riverside Information Security Standard v2.0 that laid down the policy for disaster recovery plan. Specifically, the updated standards include the most recent NIST updates for disaster recovery plan. We thank Information Technology for taking a proactive approach to establish policy for disaster recovery plan. In the follow-up audit, we will verify whether the department develops disaster recovery procedures

as per the new policy to ensure the County of Riverside Information Technology department has formally documented reviewed and evaluated disaster recovery plan."

Current Status

Reported Finding Corrected? ☐ **Yes** ☐ **No**

Partially Implemented

Recommendation 8.1

"Develop a written, formal disaster recovery plan and ensure it is formally reviewed and approved by senior management."

Management Reply

"**Concur**. RCIT is in the process of creating a formal documented Disaster Recovery Plan and plans to have the first iteration of the document completed in 6 to 9 months.

Although not formally documented, RCIT did have components of a disaster recovery plan in place prior to the audit performed by the Auditor-Controller. These items include the following:

- Backups for 60 days (there is a current project in place to increase backup availability to 365 days).
- A cloud-based disaster recovery environment that is available on demand and hyper-scalable (there are current projects in place to increase our resiliency by preparing additional cloud environments/vendors that can be leveraged in 'DR' scenarios).
- Dedicated network connections to current cloud environments (there are projects in place to create dedicated network connections to the additional cloud environments/vendors)."

Actual/Estimated Date of Corrective Action: March 1, 2025

Current Status

Corrective Action: ☐ **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 currently have DR for 200 servers in VCDR. We are currently working to implement DR for the remaining 1200+ servers (Using Wasabi Cloud Backup and Cloud Environments), which should be completed in about a year with proper funding. We are also working on implementing a DR for our PeopleSoft application in the Oracle Cloud Infrastructure. We currently have a 30-day plan (Moving out of our RC3 Data Center in 30 days), which will be used as a starting point to create a DR plan once we have implemented all of the above, which depends upon available funding.

Recommendation 8.2

"Develop a process to communicate the disaster recovery plan to appropriate stakeholders."

Management Reply

"**Concur**. The process of communicating the disaster recovery plan will be incorporated into the formal disaster recovery plan mentioned in recommendation 8.1."

Actual/Estimated Date of Corrective Action: December 1, 2025

Current Status

Corrective Action: ☐ **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).

All systems are backed up to tape at a minimum. By summer of 2025, we will have all daily backups in Wasabi, which will give us a variety of recovery options. The plan is then to expand our VCDR environment to cover the rest of the 1000 servers not covered by VCDR. However, RCIT does not have the funding to add all systems into VCDR and build extensive recovery options for all systems. RCIT will be proposing a list of critical systems and work with the Executive Office to standardize which system have basic recoverability and which systems will have more robust recovery options. Once complete, RCIT will share the recovery options with the appropriate stakeholders.

Recommendation 8.3

"Develop a process to ensure that the disaster recovery plan is annually tested for the county's critical applications, and an after-action report is developed and reviewed by senior management."

Management Reply

"**Concur**. The disaster recovery testing process will be incorporated into the formal disaster recovery plan mentioned in recommendation 8.1. RCIT manages several hundred systems and testing each of them annually would be extremely time-consuming and unpractical. RCIT will work with the Executive Office to identify the most critical systems and develop detailed plans to recover them in the event of a disaster. A general recovery plan will be developed for the remaining systems, many of which may require third-party vendor support."

Actual/Estimated Date of Corrective Action: March 1, 2025

Current Status

Corrective Action: ☐ **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 tested the DR for Laserfiche and ProLaw application in the VCDR Disaster Recovery solution. We will be testing the other applications once funding is available and we implement the solution for all our servers and the PeopleSoft applications.

Finding 9: Internal Project Cost Tracking

"Standard Practice Manual 508, *Intangible Assets – Software*, states, 'Activities involved in developing and installing internally generated computer software and the specifics of each stage can be grouped into the following steps: 1. Preliminary Project Stage: Cost activities should be expensed as incurred... 2. Application Development Stage: Cost activities should be capitalized... 3. Post-Implementation / Operation Stage: Cost activities should be expensed as occurred.' Additionally, Standard Practice Manual 508, *Intangible Assets – Software*, states, 'Capitalize expenditures if modification results in any of the following: 1. An increase in functionality... 2. Increase in efficiency... 3. Extension of estimated useful life.'

Information Technology assigned one project code to three different software modification projects. Additionally, the different phases of the software modification projects were also combined into the same project code. As such, project costs and transactions relating to the different projects and project phases were commingled under one project code. Department personnel overseeing project cost tracking were not provided adequate training or guidance over the applicable Standard Practice Manuals. Not assigning unique project codes to different software modification projects and their respective phases causes difficulties tracking dedicated internal costs related to capitalization, affecting total capitalization costs needed to remain compliant with necessary accounting standards and county policies. Additionally, it leads to inefficiencies when needing to separate costs associated with the development, implementation, and testing phases of a software development or modification project."

Current Status

Reported Finding Corrected? ☒ **Yes** ☐ **No**

Recommendation 9

"Ensure compliance with Standard Practice Manual 508, *Intangible Assets – Software*, by assigning separate project codes for each unique project and phase associated with developing or modifying internally generated computer software. This should emphasize the ability to distinguish between capitalized cost and expenditures by project."

Management Reply

"**Concur**. RCIT understands the importance of ensuring compliance with County Standards. In the future, when a CIP project has been identified (and there have been only two in over 10 years), RCIT fiscal will work with the project managers to ensure phases of the project are clearly identified and assign a program/activity code. We realize the importance of ensuring compliance with county standard codes to separate those costs into appropriate categories. RCIT has reached out to the Auditor's General Accounting unit for guidance regarding the Standard."

Actual/Estimated Date of Corrective Action: Completed

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).

RCIT has updated the internal CIP procedure to include the creation of project codes to identify the three stages of a CIP project. The Assets Manager attends monthly Procurement meetings, during which a CIP project will be identified early in the process.

Finding 10: Warranty Monitoring

"Information Technology's policy titled *RCIT Asset Disposition Notification*, Section 3.3, *Return Merchandise Authorization Procedures*, states, 'When an asset is returned to manufacturer/supplier, a Return Merchandise Authorization (RMA) Notice Form request must be submitted in [the IT service management system] to update Asset status in the inventory records.'

Ten out of sixteen (63%) warranty claims processed during the audit review period remained open after the claims were initially processed. The average days elapsed after claims processing was 260 days, with the longest processed claim remaining open for 427 days and the shortest remaining open for 68 days. The department only assigns warranty-related tasks to capital assets in the IT service management system. As such, tasks over warranty claims for non-capital assets were not finalized and closed for warranty claims in the IT service management system. Leaving the processed warranty claims open obscures the department's list of open claims by commingling processed claims with claims that have yet to be initiated. This causes time-sensitive

claims to remain open and potentially miss submission deadlines and adds to the amount of claim resubmissions that could have been avoided."

Current Status

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

Recommendation 10

"Develop a process to ensure the IT service management system is updated to reflect the actual status of warranty claims."

Management Reply

"**Concur**. When a warranty claim is submitted in the IT service management system, a task is deployed to two separate teams, the Warehouse team and the Asset team. The Warehouse team works with the vendor and the bureau to ensure the warranty claim is completed. All sixteen warranty claims were completed and closed by the Warehouse team. The Asset team also receives a task to which they confirm whether the item is a capital asset. The ten warranty claims that remained open were not closed by the Asset team because these items were not trackable assets. However, staff have now been instructed to close the task with a note referencing 'non-asset'."

Actual/Estimated Date of Corrective Action: Completed

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).

RCIT has further refined and streamlined our warranty process, developed training to educate and update staff, and established bi-weekly meetings with warranty record processors to review the status of open and recently closed tasks.