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

**ITEM**
2.18
(ID # 7822)

**MEETING DATE:**
Tuesday, August 28, 2018

**FROM :** AUDITOR CONTROLLER:

**SUBJECT:** AUDITOR-CONTROLLER: Internal Audit Report 2017-326: Riverside County Information Technology, Follow-up Audit, District: All. [$0]

**RECOMMENDED MOTION:** That the Board of Supervisors:

1. Receive and file Internal Audit Report 2017-326: Riverside County Information Technology, Follow-up Audit

**ACTION: Consent**

Paul Angulo

Paul A. Angulo, County Auditor-Controller 8/16/2018

**MINUTES OF THE BOARD OF SUPERVISORS**

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

| | |
|---|---|
| Ayes: | Jeffries, Tavaglione, Washington, Perez and Ashley |
| Nays: | None |
| Absent: | None |
| Date: | August 28, 2018 |
| xc: | Auditor |

Kecia Harper-Ihem
Clerk of the Board
By: Cecilia Gil
Deputy

| FINANCIAL DATA | Current Fiscal Year: | Next Fiscal Year: | Total Cost: | Ongoing Cost |
|---|---|---|---|---|
| COST | $0 | $0 | $0 | $0 |
| NET COUNTY COST | $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 have completed a follow-up audit of the Riverside County Information Technology. Our audit was limited to reviewing actions taken as of August 30, 2017, to correct findings noted in our original audit report 2013-011 dated November 26, 2014. The original audit report contained 13 recommendations, all of which required implementation to help correct the reported findings.

Based on the results of our audit, we found that of the 13 recommendations:

- Seven of the recommendations were partially implemented
- Six of the recommendations were not implemented

For an in-depth understanding of the original audit, please refer to Internal Audit Report 2013-011 at www.auditorcontroller.org/Divisions/AuditsandSpecializedAccounting/InternalAuditReports.

### Impact on Residents and Businesses

Provide an assessment of internal controls over the audited areas.

## SUPPLEMENTAL:

### Additional Fiscal Information

Not Applicable

**ATTACHMENT A:** Riverside County Auditor-Controller – Internal Audit Report 2017-326: Riverside County Information Technology, Follow-up Audit.

# Internal Audit Report 2017-326

# Riverside County Information Technology Follow-up Audit

## Report Date: June 13, 2018

ACO AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

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

**www.auditorcontroller.org**

**COUNTY OF RIVERSIDE**
**OFFICE OF THE**
**AUDITOR-CONTROLLER**

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

ACO AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

**Paul Angulo, CPA, MA**
**Riverside County Auditor-Controller**

**Frankie Ezzat, MPA**
**Assistant Auditor-Controller**

June 13, 2018

Dave Rogers
Chief Information Officer
Riverside County Information Technology
3450 Fourteenth Street
Riverside, CA 92501

**Subject: Internal Audit Report 2017-326: Riverside County Information Technology, Follow-up Audit**

Dear Mr. Rogers:

We have completed the follow-up audit of Riverside County Information Technology. Our audit was limited to reviewing actions taken as of August 30, 2017, to help correct the findings noted in our original audit report 2013-011 dated November 26, 2014.

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 13 recommendations, all of which required implementation to help correct the reported findings. Based on the results of our audit, we found that of the 13 recommendations:

- Seven of the recommendations were partially implemented
- Six of the recommendations were not implemented

Details of the findings from the original audit and 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 2013-011 at www.auditorcontroller.org /Divisions/AuditsandSpecializedAccounting/InternalAuditReports.

The findings in this follow-up audit report have been edited to make the report easier to understand. The context of the findings were not changed. Further, in order to safeguard the security of the county systems, we did not name the specific systems utilized by the department.

We appreciate the cooperation and assistance provided by the staff of the Riverside County Information Technology during this follow-up audit. Their assistance contributed significantly to the successful completion of the audit.

Paul Angulo, CPA, MA
Riverside County Auditor-Controller

By: René Casillas, CPA, CRMA
Chief Internal Auditor

cc: Board of Supervisors
Executive Office
Grand Jury

Internal Audit Report 2017-326: Riverside County Information Technology, Follow-up Audit

# Table of Contents

Page

Results:

# Compliance with Riverside County Information Security Policy

## Finding 1: Security Assessments Were Not Performed for Changed Security Standards

Riverside County Information Technology (Information Technology) and the seven consolidated departments have not performed required security assessments, or gap analyses, that identify the difference between the current system requirements and the new system requirements as required by Riverside County Information Security Policies (Information Security Policies). According to department information technology representatives, this occurred because they do not have the staff to perform the analysis or they were not aware of the requirement. The policy states specifically, under the Process Activity section of the Information Security Risk Management Methodology, departments must complete gap analysis within 90 days of the release of an Information Security Standard; departments will provide the Information Security Office with monthly status updates; and copies of the completed gap analysis must be provided to the Information Security Office. Information Technology's non-enforcement of Board of Supervisor's Policy A-58, *Information Security Policy* (Board Policy A-58) and the related standards relating to gap analysis could result in a breach in the county's information system.

### Recommendation 1.1

Information Technology should ensure gap analysis are completed and provided to the Information Security Office as required.

### Current Status 1.1: Partially Implemented

Information Technology has implemented advanced hardware and software for threat detection which support in analyzing Riverside County's networks and systems. New systems are analyzed for security gaps and remediated as they migrate to Riverside County Collaboration Center (RC3). However, even though Information Technology has implemented new systems to help detect system security gaps, they are still not consistently performing gap analysis for all consolidated departments. As such, we deemed this recommendation has been partially implemented.

### Recommendation 1.2

Information Technology should work in conjunction with the Information Security Office to make department staff aware of all Information Security Policy requirements.

### Current Status 1.2: Partially Implemented

A new security awareness training program has been implemented called SANS, Securing the Human. This mandatory training program for all county employees is a general overview of the Information Security Policy. However, it does not provide the specific training applicable to information technology professionals. For example, the requirements for account and access management, anti-malware, log management, device naming as well as other areas are not detailed in SANS, Securing the Human. If changes occur within Information Technology as it relates to these areas, it should be detailed in training developed specifically for information technology staff supporting these areas. Additionally, industry training is vital as information security topics change regularly.

### Recommendation 1.3

Information Security Office should actively monitor for required gap analysis reports.

### Current Status 1.3: Partially Implemented

Information Technology has implemented tools to assist in scanning and detecting vulnerabilities identified. We reviewed the reports generated from these tools to assess the information provided and found that each of these are automated. Even though these new tools were installed in the county's network to scan and detect for security gaps, regular gap analysis are not consistently performed.

## Finding 2: Security Vulnerabilities Were Not Promptly Corrected

Results of vulnerabilities identified in the information systems are not remediated within standard response time. We reviewed the vulnerability scans for Information Technology and the seven consolidated Information Technology departments for the period February 1, 2013 through June 30, 2013. For each of the departments, five servers and five workstations were selected for testing. In most instances, the risk classifications which ranged from critical to low were not remediated as directed in the standards.

Table 1 below summarizes vulnerability remediation timeframes as detailed in the Information Security Standard:

***Table 1: Vulnerability Remediation Timeframes***

| Risk Classification | Servers, Network Equipment, Storage Systems | Workstations/Mobile Workstations |
|---|---|---|
| Critical | 48 hours | 24 hours |
| Severe | 10 days | 5 days |
| Medium | 30 days | 15 days |
| Low | At discretion of DISO* | At discretion of DISO* |

**DISO – Department Information Security Officer*

Vulnerabilities are reported separately in the vulnerability scanning application for Information Technology and the consolidated Information Technology departments. From the scans performed, the departments did not remediate the vulnerabilities identified in the scans within the timeframes specified in the Information Security Standard. Table 2 summarizes the departments' number of vulnerabilities that remained un-remediated for more than a month for the systems we tested:

***Table 2: Summary Of Departments Remediation Management of Vulnerabilities***

| Department | Critical | | | | Severe | | | | Moderate | | | | Remediated Timely |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AVW | WANM | AVS | SANM | AVW | WANM | AVS | SANM | AVW | WANM | AVS | SANM | |
| Agency A | 141 | 1.2 | 245 | 3.9 | 5 | 1.8 | 12 | 3.9 | 38 | 1.3 | 84 | 3.9 | No |
| Agency B | 0 | 0 | 407 | 2 | 4 | 3 | 10 | 2 | 0 | 0 | 201 | 2 | No |
| Agency C | 456 | 2.9 | 110 | 4.6 | 7 | 1.9 | 9 | 5.4 | 121 | 2.7 | 59 | 5 | No |
| Agency D | .4 | 2 | 3 | 1.7 | 3 | 4.6 | 9 | 4.5 | 0 | 0 | .4 | 2 | No |
| Agency E | 547 | 4.6 | 35 | 3.8 | 198 | 4.7 | 13 | 4 | 14 | 4.9 | 2 | 4.2 | No |
| Agency F | 45 | 2.9 | 6 | .7 | 22 | 2.8 | 2 | 1.4 | 4 | 2.6 | 0 | 0 | No |
| Agency G | 150 | 3.5 | 248 | 4.6 | 77 | 3.8 | 366 | 4.6 | 9 | 4 | 6.8 | 4.6 | No |
| Agency H | 159 | 2 | 147 | 5 | 13 | 3.1 | 50 | 5.2 | .7 | 3.7 | 5.6 | 4.1 | No |

Legend:

| | |
|---|---|
| AVW | Average number of vulnerabilities for all workstations tested |
| WANM | Workstation average number of months vulnerabilities remained without being remediated |
| AVS | Average number of vulnerabilities for all servers tested |
| SANM | Server average number of months vulnerabilities remained without being remediated |

The causes identified by Information Technology and consolidated department information technology staff for not timely addressing vulnerabilities were:

1. Do not have the staffing resources to update and patch the systems
2. Patch management software is not available to update and patch the systems efficiently
3. Patching the vulnerabilities can be time consuming and competes with other duties
4. Some vulnerability patches require that it be done in a test environment before being placed in the production environment to identify any potential issues that may arise as a result of the patch

The Board Policy A-58 define the minimum requirements for all Riverside County information, and the systems, technologies, and processes through which information is created, acquired, processes, stored, transmitted and destroyed. Non-compliance with the minimum requirements as it relates to vulnerability management exposes the Riverside County systems and information to potential exploitation and increases the security risk.

### Recommendation 2

Information Technology and the Information Security Office should determine an appropriate manner to address vulnerabilities identified in the vulnerability scans within the timeframes allotted in the standards.

### Current Status 2: Partially Implemented

With the assets for consolidated departments in an active directory, Information Technology implemented a network platform to patch its vulnerabilities as well as third party software vulnerabilities for consolidated departments. Information Technology pushes its patches to their established test group of systems within their department, to ensure potential issues do not arise once pushed to the consolidated departments. The testing allows Information Technology to resolve any glitches prior to patch deployment to all consolidated county systems. In our review of vulnerabilities for a three-month period, we noted 2,292 vulnerabilities remain unpatched on both platforms. Considering these facts, the recommendation is partially implemented.

## Finding 3: Software to Prevent Unauthorized and Harmful Software was Not Used Appropriately

The anti-malware programs meant to protect computers and systems against viruses, spyware and other harmful external programs, are not adequately utilized by the departments. We reviewed the configurations for the anti-virus solutions and found the departments were not in compliance with anti-malware solutions which states the servers and workstations should be configured to weekly full scan, daily updates of scan engine and malware definitions, and sanitation actions set to quarantine and delete. The stated cause per Information Technology staff was that they had not been provided the revised Board Policy A-58. The standards define the minimum requirements for all Riverside County information, and the systems, technologies, and processes through which information is created, acquired, processed, stored, transmitted and destroyed. Not meeting the minimum requirements leave the Riverside County systems exposed to malware infiltrations and attacks. Table 3 summarizes the results for each department we reviewed:

***Table 3: Summary Of Anti-malware Testing Results***

| Consolidated Departments | Not Set for Full Scan | Not Reported Monthly to ISO | Not Quarantined |
|---|---|---|---|
| Agency A | ✓ | ✓ | - |
| Agency B | - | ✓ | - |
| Agency C | ✓ | ✓ | ✓ |
| Agency D | ✓ | ✓ | - |
| Agency E | ✓ | ✓ | - |
| Agency F | - | ✓ | - |
| Agency G | - | ✓ | - |
| Agency H | ✓ | ✓ | ✓ |

**Legend:**

| | |
|---|---|
| - | **Compliant with standard** |
| ✓ | **Not in compliance** |

**Note:** If during our testing, even one of the tested assets did not have the settings in accordance to the standard requirements, our conclusion was non-compliance. The logic is that one infected asset provides an access point for other systems to be infected as intended by antimalware authors.

## Recommendation 3

Formalize practices for the dissemination of standards and operational changes that includes a requirement for acknowledgment of receipt.

## Current Status 3: Partially Implemented

The SANS, Securing the Human training is a security awareness program implemented by Information Technology to educate all county staff on best security practices. The course is mandatory and requires an acknowledgement once completed by all county employees every two years. We reviewed the completion of the mandatory training for Board Policy A-58 and found that fifty-seven Information Technology employees are not current with this mandatory training.

Furthermore, we performed limited testing on the migrated servers and workstations to the technologies used to ensure consistency in policy and enforcement. These tools are designed to identify threats or unwanted software, quarantine them and report to the administrators. We reviewed the anti-malware configurations for five workstations and five servers which states each should be configured to the weekly full scan, daily updates of scan engine and malware definitions, and sanitation actions set to quarantine and delete. All were set to a different configuration than the one required. Further, three out of five servers did not meet the daily updates, malware definitions, and sanitation actions as required by the Information Security Standards.

## Finding 4: Records of Significant Computer Operations Events Were Not Maintained in Accordance with Information Security Standards

The event logs which record significant computer operation events such as user logon and logoffs, update failures and successes, program errors, and other significant events are not properly maintained for four of the eight (or 50%) departments we reviewed during our audit. According to the Information Security Standards, the logs should be maintained for a minimum of 90 days. Additionally, based on interviews with Information Technology staff and review of event log settings, we found the departments' event logs were not consistent with the standards. For example, the event logs for Transportation Land Management Agency indicated log failures but log successes were not found for audit account management, audit policy changes, audit privilege use, restart and shutdown, log on and log off, and user/group management. Also, for the Economic Development Agency, the lockout timeframe was set at 30 minutes and the standards state the timeframe should be at 60 minutes. Furthermore, for some of the log settings, log management history was set to be maintained in terms of data size and not in terms of days as indicated above. Discussions revealed that for departments not in compliance, some of the log settings for workstations and servers are left with factory settings and are left unchanged. The Riverside County Information Security Standard states that at minimum, operating systems shall be configured to audit and log system events, security events, network events, and application events. It further states that all logged events shall be retained for a minimum of ninety days. When the event logs are not properly retained or recorded, the ability to identify illegal entries into the county network system could be reduced.

## Recommendation 4.1

Information Technology should train, test and monitor department information security officers on the requirements for event logs and establish a system to confirm compliance.

### Current Status 4.1: Partially Implemented

Information Technology purchased a tool to manage all vulnerability scans, to allow its staff to view the event logs from all servers and workstations. This tool pulls from other installed auditing tools to help the Information Security Office respond to severe vulnerabilities identified in scans. We reviewed the event logs for five workstations and five servers which confirmed the logs are in accordance with standards. However, the audit function used to record log failures or successes is not enabled. With the disparity between Information Security Standards and what has been implemented, Information Technology needs to address the gap to ensure compliance with its Information Security Standards.

### Recommendation 4.2

Information Technology and the Information Security Office determine the memory capacity requirements, whether in terms of data size or in terms of days, that will satisfy the logging requirements detailed in the Information Security Standard.

### Current Status 4.2: Not Implemented

Once the tool to manage all vulnerabilities was acquired to capture event logs, the tool enabled Information Technology to report all event logs for servers and workstations. According to Information Technology officials, the capacity is set to a default memory capacity that does not meet the Information Security Standards of 90 days.

## Finding 5: Accountability of Assets is Difficult to Ascertain

The asset inventory listing of servers and workstations obtained from the consolidated department representatives did not agree with the listing extracted from the Information Security's Office's scanning software. We found assets were listed on the Information Security Office provided list (extracted from their scanning software) but not the departments provided list and vice versa. According to the department information security officers in each department, this occurs because when the monthly scans occur, often the systems, which includes servers or workstations, are powered off or are no longer in service. Furthermore, it was revealed through interviews that IP addresses, which we used to compare the lists, are commonly changed and reassigned to different information technology assets. Each department is provided with an IP address range, and all assets connected to the department's network will be assigned an IP address within the range. The Information Security Office enters the IP address range in the scanning software for the vulnerability scans. When departments assign new IP addresses to information technology assets outside the range provided to the Information Security Office, the systems outside the range are not scanned for vulnerabilities. Any new ranges need to be forwarded to the Information Security Office timely for entry into the scanning software. Not providing the updates to the Information Security Office, exposes department systems to vulnerabilities.

## Recommendation 5

Information Technology should ensure that any new IP address ranges are submitted to Information Security Office in a timely manner to ensure scan of all information technology assets.

## Current Status 5: Not Implemented

Information Technology has consolidated assets into an active directory and migrated all consolidated department assets to Riverside County Collaboration Center. An IP address management solution was purchased to assist in managing the IP address range for Information Technology. The Information Security Office redesigned their vulnerability scanning tool to configure all assets added to the active directory. Also, a configuration manager was deployed across all consolidated departments to improve reporting and location tracking of Information Technology managed assets. However, when we compared reports from the active directory and the vulnerability scanning tool we found the current IP address range had not been updated in the tool. Information Technology will need to ensure assets are updated accordingly.

## Finding 6: User Access to Information Systems Were Not Disabled Timely

We identified the following areas for improvement relating to user information account management:

- System account access for terminated or retired information technology staff were not disabled in a timely manner

- There is no written policy or procedures for disabling account access

- Departments could not provide documentation to confirm accounts were deleted

Further, 3 out of the 8 departments did not disable the account access for terminated employees in a timely manner. In discussions with department information security officers, it was stated that this was an oversight. It took 259 days to delete/remove account access for a terminated employee in one of the departments and for another department it took 330 days to disable the account.

For other departments, we found the department information security officers completely deleted the accounts without disabling them. Information Technology staff expressed that best practices would be to disable the account prior to deleting the account of the terminated/retired employee. Formal written account management practices are missing, failure to implement account management written procedures results in no accountability over the procedure.

## Recommendation 6.1

Information Technology should develop account management procedures and utilize it to train all department information security officers on the appropriate process for disabling account access.

### Current Status 6.1: Not Implemented

No revisions have been made to the account management procedures. Currently this process is completed manually with a collaboration between Information Technology and the respective departments.

### Recommendation 6.2

Establish an internal control process for disabling account access for terminated/retired employees to ensure compliance with the Information Security Standard requirements.

### Current Status 6.2: Not Implemented

The account deactivation is completed manually. A department representative notifies an Information Technology staff member of an employee termination and the account is deactivated. We selected a sample of twelve terminated county employees and found that 3 out of 12 had not been deactivated in a timely manner.

## Finding 7: Information Security Office Approval for New Systems Need to be Formalized in the Standards Conformance Review

Two of the eight departments did not obtain approval from the Information Security Office prior to implementing new systems into the county network. In both instances, we determined through interviews with information technology staff that this occurred because they did not know to submit to the Information Security Office for a conformance review or that the standard required compliance with information security specifications. All new devices should be deployed in compliance with Information Security Office established information security standards and have a conformance review performed by the Information Security Office. It is important to note that even though the Board Policy A-58 does not specifically require that new systems introduced to the Riverside County network have a conformance review performed by the Information Security Office, such practice needs to be standardized by making it a requirement under the Board Policy A-58.

### Recommendation 7

The Information Security Office should formalize the standard by including the requirements in the Board Policy A-58 if this is the desired practice.

### Current Status 7: Not Implemented

Information Technology has completed a draft of Board Policy A-58. Once they obtain approval from their internal executive team, the revised policy will be submitted to the Board of Supervisors. They project Board of Supervisors approval and implementation by July 2018. Since, the revised policy has not been approved, this recommendation has not been implemented.

## Finding 8: Awareness of Board Policy A-58 and Related Information Security Standards

Information Technology staff is not aware of Board Policy A-58 and related standards. There were instances internal audit staff was requested to provide copies of the standards being used since staff did not have copies or were not aware of requirements within the standards. It was determined through interviews with staff charged with departmental networks that there is a lack of awareness of Board Policy A-58. Information Technology staff did not know of the policies and standards governing information security lead to non-compliance with the minimum requirements for all county information, the systems, technologies, and processes through which information is created, acquired, processed, stored, transmitted, and destroyed. The Information Security Policy is a guide for departments on matters that are not otherwise addressed in state codes, county ordinances and resolutions by the Board of Supervisors. The policy also provides the framework for the Information Security Program. The Information Security Standards define the specific controls and processes required to mitigate information security risks.

### Recommendation 8

Information Technology should implement recurring training of Board Policy A-58 and ensure ongoing communication to its staff of the importance in complying with the policy and standards.

### Current Status 8: Partially Implemented

Updates to reflect the changes in Information Security Standards under Board Policy A-58 is in draft form, pending approval by their internal management and the Board of Supervisors. The department has incorporated the security requirements outlined from National Institute of Standards and Technology SP800-53 in addition to current industry best practices in their revision. Information Technology implemented SANS, Securing the Human training course, for all county employees. This training is required to be completed every two years. In the modules, there are options to complete the SANS, Securing the Human training for general users, information technology administrators, and criminal justice. The revisions made in the draft are currently not reflected in the SANS, Securing the Human training. Further the information technology administrator's modules includes topics such as work in remedy, help desk, personally identifiable information and information technology staff which does not address specific controls and processes required.

## Business Continuity & Physical Security of Network

### Finding 9: Disaster Recover

Information Technology stated they utilize their disaster recovery plan which does not focus on best practices for business continuity plan areas such as weekly data back-ups, restoring from back-up status, annual testing of the plan, detailed arrangements for immediate replacement of essential hardware, and written processes for restoration of backed up data. With a new Chief Information Officer at the helm, the department has been in the process of revising the disaster recovery plan to address the areas identified for a business continuity plan. Without an actionable plan in place the county may be exposed to internal and external risk.

### Recommendation 9

Information Technology should complete a business continuity plan and submit to the Board of Supervisors for approval as early as possible.

### Current Status 9: Not Implemented

Information Technology has not prepared a comprehensive business continuity plan. It plans to create one after the consolidation to Riverside County Collaboration Center, the Riverside County's centralized tier 3 data center. Full implementation for this recommendation is expected to occur December 2018.

It is important to note that for the better part of a decade this has been under plans and discussions. It is critical for Information Technology to pursue this with priority as disasters can strike at any moment without warning.

**DAVE ROGERS**
ACEO, Chief Information Officer

**JIM SMITH**
Chief Technology Officer

RCIT

**LOUIS RAJA ARUL DOSS, ACIO**
Enterprise Applications Bureau

**PATRICK ELLIANO, ACIO**
Converged Communications Bureau

**GIL MEJIA, ACIO**
Technology Services Bureau

## MEMORANDUM

TO: Paul Angulo, Auditor-Controller

FROM: Jim Smith, Chief Technology Officer JS

DATE: August 14, 2018

RE: Response to Internal Audit Report 2017-326

---

On November 26, 2014, the Auditor-Controller's Office (ACO) submitted Internal Audit Report 2013-011 to the Board of Supervisors. The intent of this audit was to review Riverside County Information Technology (RCIT) and its compliance against Board Policy A-58, which included 13 detailed findings and their recommendations to remediate them. On June 13, 2018, the ACO submitted to RCIT the results of a follow-up to their original audit to determine the remediation status of the recommendations proposed in their initial 2014 report. In the follow-up report, the ACO concluded that seven of their recommendations were "Partially Implemented" and that the remaining six were "Not Implemented." While RCIT agrees that several of the findings are technically accurate, we feel that context and background information must be added to understand why all the ACO recommendations have not yet been "Fully Implemented." Additionally, RCIT would like to outline the measures that we have put in place to address several of the recommendations and show that we are taking the steps necessary to address all of the ACO's security concerns.

Information Technology has changed substantially over the last decade. Many of the policies and settings that were appropriate in the past are not applicable today. The current A-58 policy was written in 2009 and is very outdated by today's standards. RCIT has been working on a new A-58 policy that we will bring to the Board for approval later this year. This new policy is based on current recommendations from the National Institute of Standards and Technology, an agency under the U.S. Department of Commerce dedicated to developing and maintaining a variety of national technical standards. This new policy will better fit the current requirements of Riverside County and will be updated regularly in collaboration with departmental security personnel.

When the initial ACO audit was performed in 2013, the consolidation of countywide IT resources under RCIT had just begun, and was mostly on paper. At that time, RCIT managed the IT resources for seven departments. However, in July of 2014, RCIT assumed the responsibility for infrastructure belonging to an additional 21 agencies bringing the total number of supported departments to 28. What RCIT found as we began the discovery process inside these agencies was that most of their technology environments were in various stages of decay due to a lack of funding and an insufficient set of departmental IT skills to manage all facets of their IT infrastructure and applications. As many as 400 servers were not being backed up sufficiently, or at all. Most of the IT infrastructure was at or beyond its useful life and not covered by any form of support, and most computer rooms did not have adequate cooling or power protection. As a result, RCIT has spent a significant amount of time since 2014 in a reactive mode to keep departmental applications and services up and running.

In July of 2015, RCIT brought in a new executive leadership team to address the lack of progress being made towards IT consolidation. To make any substantial progress towards the consolidation of IT resources, the new leadership team chose to focus primarily on perimeter and network security rather than the individual remediation of 28 different environments. A significant investment was made in world-class security products such as Tipping Point (IDS/IPS), Splunk (Enterprise Logging), InTune (Mobile Device Management), Securi (Web

Application Proxy), and NetWitness (Packet Inspection). These products provided an immediate enterprise security umbrella around the County's IT infrastructure, allowing RCIT the time to work on the detailed security remediation of the network and our endpoints.

RCIT's overall strategy is to focus on building new enterprise environments and migrating departments into them rather than remediating deficiencies within the aging departmental systems. This approach is resulting in the simultaneous remediation of risk AND the upgrade of departmental systems into a modern environment that is current, secure, and located inside a fault-tolerant ecosystem at the county's enterprise data center, RC3. In addition, RCIT has been able to identify redundant and/or unnecessary systems. Thus far, RCIT has eliminated twenty-five percent (25%) of the departmental servers, which further reduces the county's overall security risk.

As we head into the final phases of IT consolidation, we estimate another twelve months before all desktops belonging to the consolidated departments will be migrated into the enterprise Active Directory and most servers moved to RC3. This consolidation of resources will allow RCIT to manage and maintain one set of standardized security rules and policies across more than 10,000 desktops and 1,000 servers, rather than attempting to create and maintain the same security standards across 28 different environments.

As for the ACO findings, RCIT would like to address a few of the most significant items and add information that will put them into context with the "bigger picture" and build confidence that RCIT understands the issues, is prioritizing them properly, and has made considerable strides in the right direction.

**Finding #2 – Security Vulnerabilities Were Not Promptly Corrected (Partially Implemented)**

There are two major RCIT concerns with this finding as it relates to policy A-58:

1. RCIT recognizes that it is important to apply security patches as quickly as is reasonably possible. However, the key word is "reasonably." Almost all security patches are released to plug "theoretical" vulnerabilities that do not have any known published exploit at the time they are published. These vulnerabilities do not pose a risk until malware is developed to exploit them, which in many cases never happens. Rushing to patch these vulnerabilities can have unintended consequences and cause more serious problems than the malware they are intended to prevent. It is imperative to evaluate each patch, determine its applicability, and properly test it on a sampling of systems prior to deploying it to every system across the county. While most patches are reversible, some are not. Prematurely deploying a flawed patch throughout the county could cause catastrophic results. It is RCIT's policy to apply all security patches regardless of their severity level within 24 hours of their release to a select group of systems that pose a low risk if the patch does not work as expected. These systems are evaluated for a week, and if successful are deployed to the remaining systems through an automated process. If a vulnerability is serious enough AND there is active malware to exploit it, then RCIT will deploy the patch to all systems within 24 hours, or provide an alternative solution that mitigates the vulnerability at a policy or global network level.

2. RCIT staff receive Rapid 7 reports on a regular basis from our Security Office. These reports list the Top 25 vulnerabilities within each of the RCIT supported departments. The number one problem in each department is not with the Microsoft patches, but rather with Oracle Java, Adobe Acrobat, and Adobe Flash. These three applications account for more than 75% of the estimated endpoint risk in Riverside County. However, in most cases, they cannot be upgraded due to departmental application dependencies that would break if patched. RCIT continues to work with agencies to determine these dependencies and make recommendations to either upgrade their applications or migrate to a platform that does not rely on Oracle or Adobe plugins. Remediating these applications may also

require departments to fund the remediation process or purchase new applications to replace the legacy application.

### Finding #5 – Accountability of Assets is Difficult to Ascertain (Not Implemented)

According to the follow-up audit "***Compared the IP addresses and found more IP addresses in Rapid 7 than what was identified in Active Directory.***" There will always be more IP addresses in Rapid 7 than in Active Directory. This is by design and used for historical reporting purposes. Rapid 7 scans the entire network once each month. However, Active Directory is dynamic and changes daily. If there had been more addresses in Active Directory than Rapid 7, then there would have been a gap that would need remediating. In this case, RCIT considers this finding "Fully Implemented."

### Finding #6 – User Access to Information Systems Were Not Disabled Timely (Not Implemented)

This is not a technology problem. This is a process problem that needs to be addressed between the departments, Human Resources, and RCIT. As of July 2016, all departments have access to ServiceNow (RivCo Help) which is used to add/move/terminate employees. Although most departments are sending their requests prior to an employee leaving the County, some departments submit their requests late or not at all. RCIT can only disable an account properly if departments report the termination to us in a timely manner.

Ultimately, the disabling of accounts from the HR system would be ideal, but this cannot be accomplished until all accounts are in the enterprise Active Directory (RIVCOCA). Until then, we must rely on the departments or HR to inform us when an employee leaves the County. In the interim, RCIT is working with Human Resources to run a regular report of terminated employees so that we can verify that accounts and any other rights associated with a terminated employee are disabled in a timely manner.

### Summary

RCIT has made a tremendous amount of progress consolidating, upgrading, and securing the County's IT assets over the last three years. We recognize that there is still a lot of work to be done and are committed to completing it as quickly as possible and with minimal user interruption. We are confident that the full consolidation of all RCIT supported resources will be complete within the next twelve to eighteen months, which includes the elimination of departmental "resource forests." In the meantime, we will continue to work with departments to upgrade their legacy applications, remediate security gaps, and improve our security-related processes.

We look forward to our continued work with the ACO to improve the security of the County's IT infrastructure and protect the integrity of our data.