PUBLIC INFORMATION

# INTERNAL AUDIT DEPARTMENT

## Second & Final Close-Out Follow-Up Information Technology Audit: Auditor-Controller Information Technology General Controls

**As of December 31, 2020**

**Audit No. 2059-F (Reference 1741-F2)**
**Report Date: October 14, 2021**

### Recommendation Status

| FIRST FOLLOW-UP | | SECOND FOLLOW-UP |
|---|---|---|
| 1 | Implemented | 11 |
| 11 | In Process | 0 |
| 0 | Not Implemented | 0 |
| 0 | Closed | 0 |

Second Follow-Up totals represent findings that were In Process or Not Implemented at First Follow-Up

## OC Board of Supervisors

| CHAIRMAN ANDREW DO | VICE CHAIRMAN DOUG CHAFFEE | SUPERVISOR KATRINA FOLEY | SUPERVISOR DONALD P. WAGNER | SUPERVISOR LISA A. BARTLETT |
|---|---|---|---|---|
| 1st DISTRICT | 4th DISTRICT | 2nd DISTRICT | 3rd DISTRICT | 5th DISTRICT |

PUBLIC INFORMATION

# INTERNAL AUDIT DEPARTMENT

Audit No. 2059-F
(Reference 1741-F2)

October 14, 2021

To: Frank Davies, CPA
Auditor-Controller

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

Subject: Second & Final Close-Out Follow-Up Information Technology Audit: Auditor-Controller Information Technology General Controls

---

We have completed a second follow-up audit of Auditor-Controller's information technology general controls as of December 31, 2020, original Audit No. 1741, dated March 6, 2019. Due to the sensitive nature of specific findings (restricted information), only the results for Finding Nos. 3, 11, and 12 immediately follow this letter. Results for the remaining findings are included in Appendix A (which is redacted from public release), and additional information including background and our scope is included in Appendix B.

Our second follow-up audit concluded Auditor-Controller implemented the eleven (11) remaining recommendations. Because all our recommendations were implemented, this report represents the final close-out of the original audit.

We appreciate the assistance extended to us by Auditor-Controller personnel during our follow-up audit. If you have any questions, please contact me at 714.834.5442 or Assistant Director Scott Suzuki at 714.834.5509.

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
Auditor-Controller Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Eide Bailly LLP, County External Auditor

## RESULTS

| | |
|---|---|
| **FINDING NO. 1** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 2** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 3** | **Change Management Process** |
| **CATEGORY** | **Critical Control Weakness** |
| **RECOMMENDATION** | We recommend Auditor-Controller create and implement formal change management processes including:<br>1) Documenting proper management review, approval, and testing of changes prior to deploying changes into the production environment.<br>2) Limiting vendor access to the department's production environment, where feasible.<br>3) Considering creation of a departmental change advisory/review board with periodic meetings to ensure that all changes are discussed, reviewed, approved, and documented prior to deployment into production. For emergency changes, the board should ensure changes are reviewed post-implementation. |
| **CURRENT STATUS** | **Implemented.** Auditor-Controller developed policy and procedures over change management including configuration and change management processes, software migration processes, and identity management.<br><br>Vendor access has been reviewed and limited to terminal server access, which prevents direct access to the Auditor-Controller network domain. Current vendor access to VTI is provided upon request by the vendor and this access is captured in the virtual private network & remote desktop protocol logs.<br><br>Lastly, Auditor-Controller has implemented a daily operations meeting to inform staff of upcoming changes to critical systems and significant items are reported to executive management.<br><br>Based on the actions taken by Auditor-Controller, we consider this recommendation implemented |

| | |
|---|---|
| **FINDING NO. 4** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 5** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 6** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 7** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 8** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 9** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 10** | Removed due to the sensitive nature of the finding. |

| | |
|---|---|
| **FINDING NO. 11** | **Data Backup Tape Inventory Utility Access** |
| **CATEGORY** | **Control Finding** |
| **RECOMMENDATION** | We recommend Auditor-Controller timely remove access for employees who are no longer with Auditor-Controller IT or whose primary job duties no longer involve backups. Further, we recommend Auditor-Controller periodically review access to the backup tape inventory utility to ensure that access is appropriately assigned to individuals with a direct business need. |
| **CURRENT STATUS** | **Implemented.** Auditor-Controller reviewed its backup job tape inventory utility online portal and removed access for personnel that did not require access to the backup tapes. Auditor-Controller also indicated that they would utilize the user certification process they developed for the backup utility listing going forward.<br><br>Based on the actions taken by Auditor-Controller, we consider this recommendation implemented |

| | |
|---|---|
| **FINDING NO. 12** | **Privileged New User Access Documentation** |
| **CATEGORY** | **Control Finding** |
| **RECOMMENDATION** | We recommend Auditor-Controller properly document management authorization and requests for privileged new user access to network resources. |
| **CURRENT STATUS** | **Implemented.** Auditor-Controller developed a formal process for requesting privileged user access rights to critical systems that require a review of stakeholders and management authorization before granting such access rights.<br><br>Although there were no requests for privileged user access in our follow-up audit period, the enhanced controls implemented provide reasonable assurance that future privileged access requests will be properly documented with management's authorization.<br><br>Based on the information and documentation reviewed, we consider this recommendation implemented. |

| | | |
|---|---|---|
| **AUDIT TEAM** | Scott Suzuki, CPA, CIA, CISA, CFE | Assistant Director |
| | Jimmy Nguyen, CISA, CFE, CEH | IT Audit Manager II |
| | Scott Kim, CPA, CISA, CFE | IT Audit Manager I |
| | Stephany Pantigoso | Senior Auditor |
| | Mari Elias, DPA | Administrative Services Manager |

## APPENDIX A: RESTRICTED INFORMATION

Content in Appendix A has been removed from this report due to the sensitive nature of the specific findings.

## APPENDIX B: ADDITIONAL INFORMATION

| | |
|---|---|
| **SCOPE** | Our second follow-up audit was limited to reviewing actions taken by Auditor-Controller as of December 31, 2020 to implement the remaining eleven (11) recommendations from our first follow-up Audit No. 1949-A, dated May 29, 2020. |
| **BACKGROUND** | The original audit reviewed selected information technology general controls administered by Auditor-Controller as of February 28, 2018.<br><br>The original audit identified four (4) Critical Control Weakness, four (4) Significant Control Weaknesses, and four (4) Control Findings. |

## APPENDIX C: FOLLOW-UP AUDIT IMPLEMENTATION STATUS

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