PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Second Follow-Up
Information Technology Audit:
County Executive Office/
OC Information Technology
General Controls

As of February 29, 2020

Audit No. 1949-F (Reference 1644-F2)
Report Date: March 11, 2021

Recommendation Status

FIRST FOLLOW-UP		SECOND FOLLOW-UP
18	Implemented	9
12	In Process	3
0	Not Implemented	0
1	Closed	0

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

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 1949-F
(Reference 1644-F2)

March 11, 2021

To: Joel Golub
Chief Information Officer

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

Subject: Second Follow-Up Information Technology Audit: County Executive Office/OC Information Technology General Controls

We have completed a second follow-up audit of the IT General Controls administered by the County Executive Office/OC Information Technology (OCIT) as of February 29, 2020, original Audit No. 1644, dated April 10, 2018. Due to the sensitive nature of specific findings (restricted information), only the results for Finding Nos. 9, 11, 20, 23, 25 and 31 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 OCIT implemented nine (9) recommendations of the 12 remaining recommendations and is in the process of implementing three (3) recommendations. The three (3) recommendations not yet fully implemented will be brought to the attention of the Audit Oversight Committee at its next scheduled meeting.

We appreciate the assistance extended to us by OCIT 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
CEO Distribution
OCIT Distribution
Robin Stieler, Clerk of the Board of Supervisors
Foreperson, Grand Jury
Eide Bailly LLP, County External Auditor

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

RESULTS

FINDING NO. 2	Removed due to the sensitive nature of the finding.
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. 9	**Terminated Access Not Properly Documented**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT: 1) Enhance the process of monitoring and maintaining County contractor employment activities to ensure that accurate and detailed employee information (e.g., employee start/end date, job title) is appropriately recorded within the in-house application for County vendor employees. 2) Ensure an IT helpdesk ticket is submitted by business management or a delegate, upon employee termination, as support documentation to show evidence that IT was appropriately notified of termination, in order to process the request of disabling access to network resources for Shared Services. 3) Consider setting expiry dates for contractor logical access where possible.

CURRENT STATUS & PLANNED ACTION	**In Process.** OCIT adopted ServiceNow as the IT service management system (SMS) to manage and track provisioning and de-provisioning of network user access request process. As part of our testing, we selected and reviewed a sample of employee terminations that occurred during the follow-up audit period to verify that authorization for disabling user access was appropriately documented in SMS. Out of 15 employee terminations selected across Managed and Shared Services separations, five (33%) did not have appropriate support documentation to verify the recommendation was met. In some cases, the support documentation was not created timely or there was no support documentation available. OCIT has indicated they are in the process of deploying Microsoft Identity Management (MIM) software, which is designed to provide more effective end-to-end management of network user account lifecycles. Furthermore, it will automate the process of deprovisioning Shared Services and Managed Services employee network user and contractor accounts upon separation. Based on the actions taken by OCIT, including that the MIM solution has not been fully deployed, we consider this recommendation to be in process.

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

FINDING NO. 11	**New User Access Lacked Management Approval**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT ensure requests for new user access to network resources are appropriately authorized by management and documented prior to provisioning access.

CURRENT STATUS & PLANNED ACTION	**In Process.** OCIT adopted ServiceNow as the IT service management system (SMS) to manage and track provisioning and de-provisioning of network user access request process. As part of our testing, we selected and reviewed a sample of 15 employees that were hired across OCIT Shared and Managed Services during the follow-up audit period to verify whether an SMS helpdesk ticket was submitted, and appropriate authorization was documented prior to provisioning new network user accounts. For seven of the 15 (47%) reviewed, OCIT was unable to provide support documentation in SMS as evidence that appropriate authorization was documented. OCIT has indicated they are in the process of deploying Microsoft Identity Management (MIM) software, which is designed to provide more effective end-to-end management of network user account lifecycles. Furthermore, it will automate the process of provisioning Shared Services and Managed Services employee network user and contractor accounts. Based on the actions taken by OCIT, including that the MIM solution has not been fully deployed, we consider this recommendation to be in process.

FINDING NO. 20	**Shared Services Lacks Service Level Agreements/Requirements with Client Departments**
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	We recommend OCIT Shared Services develop standardized SLAs (Service Level Agreements) and/or SLRs (Service Level Requirements) for services provided across all Shared Services departments to enable monitoring of performance.
CURRENT STATUS	**Implemented.** OCIT Shared Services developed standardized SLAs and SLRs for services provided across all OCIT Shared Services departments and implemented these requirements into ServiceNow, the IT Service Management System (SMS). We noted, through the SMS, that appropriate OCIT personnel are automatically notified via email when a specific SLA/SLR has passed a critical threshold or is breached. Based on the actions taken by OCIT, we consider this recommendation to be implemented.

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

FINDING NO. 23	**Backup Jobs Schedule Not Current**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT Shared Services follow documented procedures for quarterly review of scheduled backup jobs and ensure all changes are reviewed and authorized. Furthermore, management should periodically review all backup tools and ensure they are set up with current data, and re-run all abended backup jobs to successful completion.
CURRENT STATUS	**Implemented.** OCIT Shared Services developed documented procedures for quarterly review of scheduled data backup jobs, and for the review and authorization of changes made to those jobs. We verified that the quarterly review was followed in accordance to OCIT's documented procedures. In addition, management periodically reviewed all data backup software to ensure they are set up with current backup schedules and abended backup jobs were re-run to completion. Based on the actions taken by OCIT, we consider this recommendation to be implemented.

FINDING NO. 25	**Redundant Backup and Incident Management Solutions**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT continue its plan to consolidate the backup and incident management tools to reduce redundancies, gain cost savings, and manage Shared Services resources more effectively.
CURRENT STATUS	**Implemented.** • OCIT has consolidated data backup software solutions with all OCIT Shared Services departments from the original audit (excluding departments that joined the Shared Services model subsequent to the original audit) and Shared Services is now utilizing a data backup software solution. • OCIT has successfully consolidated incident management solutions and Shared Services has implemented ServiceNow as the IT Service Management System (SMS) for its centralized incident management solution. Based on the actions taken by OCIT, we consider this recommendation to be implemented.

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

FINDING NO. 31	**County IT Policy, Procedures, Standards, and Guidelines Are Outdated**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT adopt the County's process to manage and maintain policies, procedures, standards, and guidelines so they are relevant. Additionally, continuous monitoring should be incorporated to make necessary changes as they relate to evolving new technologies.
CURRENT STATUS	**Implemented.** OCIT informed us it contracted a reputable cybersecurity third-party vendor to assist with developing new Information Technology (IT) policies, as well as revise existing policies to meet industry best practices. OCIT established the Cyber Security Joint Task Force (CSJTF) and developed a uniform County Cybersecurity Policy dated February 25, 2020. In addition, OCIT adopted the NIST 800-53 Cybersecurity standards and practices framework. Lastly, OCIT created a SharePoint intranet site titled "County Policy Library" designed as a policy repository to maintain various finalized policies and procedures, such as Cybersecurity and Patch Management. The site is accessible to all County personnel. Based on the actions taken by OCIT, we consider this recommendation to be 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
	Mari Elias, DPA	Administrative Services Manager

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

APPENDIX A: RESTRICTED INFORMATION

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

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

APPENDIX B: ADDITIONAL INFORMATION

SCOPE	Our second follow-up audit was limited to reviewing actions taken by OCIT as of February 29, 2020 to implement the remaining 12 in-process recommendations from our first follow-up Audit No. 1748-A, dated June 26, 2019.
BACKGROUND	The original audit reviewed information technology general controls administered by OCIT for the year ended December 31, 2016 to ensure physical and logical security to data and programs, change management and system development life cycle processes, and computer operations are appropriate, approved, managed, maintained, and adequately supported. In addition, we conducted a review of OCIT's implementation of selected components of the IT governance model. The original audit identified six (6) Critical Control Weaknesses, eight (8) Significant Control Weaknesses, and 17 Control Findings.

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

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.