PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

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

As of November 30, 2018

Audit No. 1748-A (Reference 1644-F1)
Report Date: June 26, 2019

Recommendation Status

18	Implemented
12	In Process
0	Not Implemented
1	Closed

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 1748-A
(Reference 1644-F1)

June 26, 2019

To: Joel Golub
Chief Information Officer

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

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

---

We have completed a follow-up audit of the IT General Controls administered by the County Executive Office/OC Information Technology (OCIT) as of November 30, 2018, 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 to 20, and 22 to 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 First Follow-Up Audit concluded that OCIT implemented 18 recommendations, is in the process of implementing 12 recommendations, and one recommendation is closed. A second follow-up audit will be performed in approximately six months and a follow-up audit report form is attached to facilitate this audit. Any recommendations not implemented at that time will be brought to the attention of the Audit Oversight Committee at its next scheduled meeting.

We appreciate the assistance extended to us by County Executive Office/OC Information Technology 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
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Vavrinek, Trine, Day & CO., 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	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. 8	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 amended contracts with its IT vendors to add a Service Level Requirement (SLR) that financially penalizes the vendors if they do not properly report their employee employment status data timely. As a result of these amendments, this process has significantly improved the assurance that IT vendors perform duties in accordance with the SLR regarding proper oversight of user de-provisioning access to County network resources. OCIT Shared Services has also adopted ServiceNow (SMS) as the service management tool to manage and track de-provisioning of network user access requests. However, SMS has not been fully deployed. OCIT is going through a wide-scale transition of consolidating IT vendor functions for its Managed Services. Since portions of our recommendation involve OCIT Managed Services, we will test these areas during our second follow-up, once the transition is complete. Based on the actions taken by OCIT, 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.** As noted earlier, OCIT Shared Services has adopted SMS as the service management tool to manage and track provisioning and de-provisioning of network user access requests. However, SMS has not been fully deployed. OCIT is going through a wide-scale transition of consolidating IT vendor functions for its Managed Services. Since portions of our recommendation involve OCIT Managed Services, we will test these areas during our second follow-up, once the transition is complete. Based on the actions taken by OCIT, we consider this recommendation to be in process.

FINDING NO. 12	**Countywide IT Security Policy Does Not Address Certain Password Security Settings**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT: 1) Enhance the Countywide IT Security Policy to enforce a more robust password configuration management policy that meets current best business practice, such as password history and lockout threshold. 2) Review password configuration rules annually to ensure they continue to adhere to the County IT Security Policy.

CURRENT STATUS	**Implemented.** The Cybersecurity Best Practice Manual was developed by the County Cybersecurity Joint Task Force (CSJTF). The manual was approved by the IT Executive Council and distributed Countywide in September 2018. The manual includes guidance on key requirements for applying more robust password configurations to critical systems that meet current best practices. While the Countywide IT Security Policy is being revised, OCIT has taken other Countywide corrective action such as issuing a memo to address the importance of applying proper password complexity requirement settings as well as performing a review of network password configurations for Shared Services. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 13	**Current Antivirus Software Not Installed on System Component**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT perform a frequent and robust review of system components to ensure all system components connected to the County network domain, including the Disaster Recovery Site in [redacted] are installed with the most current antivirus/malware software and definitions to reduce the risk of a virus and/or malware attack as recommended by the vendor.
CURRENT STATUS	**Implemented.** The original finding pertained to the County's Disaster Recovery Site. Accordingly, OCIT appropriately modified the configuration to its antivirus/malware central management software to ensure all system components located at the off-site disaster recovery site are properly managed. As a result of the modifications, the system component located at the off-site disaster recovery site was installed with the most current antivirus/malware software and updates to reduce the risk of malware attacks, as recommended by the vendor. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 14	**Change Request Risk Assessment Not Consistently Completed**
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	We recommend OCIT Managed Services complete changes to the programming of the change-management monitoring tool to ensure a risk assessment is completed and submitted with a change request.
CURRENT STATUS	**Implemented.** OCIT properly completed and submitted a risk assessment with each change request. In addition, all change requests were appropriately reviewed during weekly Change Advisory Board (CAB) meetings and denied if a risk assessment was not performed. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 15	**Shared Services Change Management Tool Lacked Critical Information**
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	We recommend OCIT Shared Services enhance the change-management tool to ensure critical information is included in the current change-management tool such as status, timestamps, and CAB reviews and approvals.
CURRENT STATUS	**Implemented.** OCIT Shared Services has implemented ServiceNow (SMS) as the IT service change management tool to manage and track changes to its computing environment at departments. SMS includes critical information such as status of the change request, timestamps for actions taken such as management approvals, and CAB meeting dates. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 16	**Application Cloud Migration Strategy Not Finalized**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT finalize the Application Cloud Migration Strategy and ensure appropriate documentation is created and maintained for all application migrations into the Cloud.
CURRENT STATUS	**Implemented.** OCIT management finalized and approved the "Application Cloud Migration Strategy" document. Although there were no application migrations to the cloud to test during our follow-up audit period, OCIT indicated this policy will be enforced for future application cloud migrations. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 17	**Emergency Changes Were Not Reviewed After Implementation**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT Managed Services ensure the additions to the CAB agenda for emergency changes includes review and approval, and becomes an integral part of the weekly CAB meetings.
CURRENT STATUS	**Implemented.** OCIT appropriately reviewed and approved emergency changes in CAB meetings. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 18	**Programming Standards Not Documented**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT develop and formalize a documented programming standard that is consistent across all applications.
CURRENT STATUS	**Implemented.** OCIT finalized and implemented a standards document titled "Application Development Standards". This document defines guidelines to enforce consistent programming standards across County IT systems. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 19	**System Development Life Cycle Procedures Not Documented**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT update their written SDLC (Software Development Life Cycle) procedures and ensure appropriate documentation is reviewed and authorized for all new application/systems that are acquired, modified, or developed to ensure consistency with the SDLC.
CURRENT STATUS	**Implemented.** OCIT updated its documented SDLC Policy to include procedures for the preparation, review, and authorization of appropriate documentation for new application and systems acquired, modified, or developed. Based on the actions taken by OCIT, we consider this recommendation implemented.

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 & PLANNED ACTION	**In Process.** OCIT Shared Services has developed standardized SLAs and SLRs for services provided across all OCIT Shared Services departments. However, OCIT has not finalized or implemented the SLAs and SLRs. OCIT Shared Services indicated they submitted a request to SAIC to implement the changes into ServiceNow (SMS) to enable the SLAs and SLRs to be monitored and tracked. Based on the actions taken by OCIT, we consider this recommendation to be in process.

FINDING NO. 21	Removed due to the sensitive nature of the finding.

FINDING NO. 22	**Error Messages Not Configured For Abended Backup Jobs**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT Shared Services maintain the enabled status on the backup tool that notifies computer operators if a job abends. Additionally, management should periodically review all backup tools and ensure they are set up to timely notify appropriate staff of any backup job failures that occur.
CURRENT STATUS	**Implemented.** OCIT enabled alert features to notify the appropriate computer operator of backup job abends (termination of job before completion). In addition, OCIT developed a policy titled "Backup & Restore Guideline," which outlines management's responsibility for performing quarterly reviews to ensure notifications are issued to the proper computer operators. Based on the actions taken by OCIT, we consider this recommendation implemented.

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 & PLANNED ACTION	**In Process.** OCIT Shared Services developed documented procedures for quarterly review of scheduled backup jobs, and review and authorization of changes made to those jobs. While the procedures documented the process for management review, the last available evidence of reviews being performed was May 2017. Based on the actions taken by OCIT, we consider this recommendation to be in process.

FINDING NO. 24	**Escalation Procedures for Incident Management Not Documented**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT implement and follow its escalation procedures, and update the procedures for any significant changes.
CURRENT STATUS	**Implemented**. OCIT finalized and approved a documented incident management process. This process included guidelines for determining the impact and urgency of an incident and varying escalation procedures. 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 & PLANNED ACTION	**In Process.** • The consolidation of a data backup solution has been completed with the exception of OC Community Resources (OCCR) and Child Support Services (CSS). OCIT will migrate OCCR's physical server data to virtual machines, before it can migrate backup jobs onto the consolidated backup solution, and at CSS, there is currently no budgeted funding so the backup solution is not scheduled for consolidation at this time. • The consolidation of incident management solutions has not been completely implemented. OCIT Shared Services has implemented ServiceNow (SMS) for its centralized incident management tool, except for the Probation Department which is expected to be implemented by quarter one or two of Fiscal Year 2019-20. Based on the actions taken by OCIT, we consider this recommendation to be in process.

FINDING NO. 26	**Cybersecurity Framework Not Fully Implemented**
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	We recommend OCIT fully implement a cybersecurity framework, inclusive of a comprehensive cybersecurity program, that is approved by the Board of Supervisors for Countywide application.
CURRENT STATUS	**Implemented.** OCIT established a Cybersecurity Joint Task Force (CSJTF) that includes members from various County departments. The CSJTF developed the Security Policy Guideline and minimum requirements for departments to create their own cybersecurity program. The minimum requirements establish a common set of standards and practices to improve and enhance the cybersecurity posture for all County departments. The cybersecurity program requirements are based on the Department of Homeland Security Cyber Resilience Review (CRR). The CRR cross references with the National Institute of Standards and Technology (NIST) Cybersecurity Framework – Identify, Protect, Detect, Respond and Recover. As a result of the CSJTF, a Cybersecurity Best Practice Manual was developed, approved by the IT Executive Council, and distributed Countywide in September 2018. The Cybersecurity Best Practice Manual details the establishment of a common set of standards and practices to improve and enhance the cybersecurity posture for all County departments. The Cybersecurity Manual addresses topics such as: • Program Roles and Responsibilities • Programs (cybersecurity, privacy, public records act, and e-discovery) • Administrative Controls (policies in compliance with CRR) • Technical Controls (e.g., mobile device management settings, group policy) • Operational Controls (processes to implement policies) Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 27	**Security Risks From Lack of Countywide IT Security Authority**
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	We recommend OCIT define specific areas where they believe they should have critical authority and influence, and seek CEO and Board of Supervisors approval. For departments with IT functions not managed by OCIT, formal communication and ad hoc meetings with Technology Council members should be organized to ensure network configuration and security of interconnected environments is quickly addressed to minimize risks. All members within the Technology Council should be provided the changes necessary to harden the network infrastructure. A validation of this process should be performed by the Cyber Resilience group to ensure management adheres to, and is in compliance with, the proposed changes required.
CURRENT STATUS	**Implemented.** OCIT has established the Cyber Security Joint Task Force (CSJTF) to develop the minimum requirements for departments to create their own cybersecurity programs. The CSJTF was created under the IT Executive Council to gain security authority to address the increasing threats to the security of County data and information systems. In addition, the CSJTF is comprised of Countywide IT personnel from various departments who meet and discuss cyber-security matters monthly. As a result of the CSJTF, a Cybersecurity Best Practice Manual was developed, approved by the IT Executive Council and the County Executive Officer, and distributed Countywide in September 2018. The Cybersecurity Best Practice Manual details the establishment of a common set of standards and practices to improve and enhance the cybersecurity posture for all County departments. The manual applies to all County departments because the County Cyber Resilience Group will be responsible for providing cybersecurity assessments for appointed and elected departments. Based on the actions taken by the OCIT, we consider this recommendation implemented.

FINDING NO. 28	**Lack of Comprehensive IT Risk Management Framework**
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	We recommend OCIT continue to develop a comprehensive IT risk management framework that incorporates all risk areas including areas outside cybersecurity.
CURRENT STATUS	**Implemented.** OCIT has established the Cyber Security Joint Task Force (CSJTF) to develop the minimum requirements for departments to create their own cybersecurity programs. Departments perform a cybersecurity self-risk assessment annually, and the results are collected and compiled by OCIT in a secured Government, Risk & Compliance (GRC) software for analysis. As a result of the CSJTF, a Cybersecurity Best Practice Manual was developed, approved by the IT Executive Council, and distributed Countywide in September 2018. The Manual outlines the County's adoption of the National Institute of Standards and Technology (NIST) Cybersecurity framework that includes risk management best practice procedures. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 29	**Incomplete Application Procurement Documentation**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT ensure documentation required by the Countywide IT Governance Strategy is prepared to evidence analysis and rationale, proper authorization, review, and approval for key decisions relating to application procurement.
CURRENT STATUS	**Implemented.** The OCIT application procurement process appropriately includes the requirement of analysis and rationale, proper authorization, review, and approval. While there were no large IT procurements to test during our follow-up audit period, OCIT indicated this process will be enforced for future IT application procurements. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 30	**Non-Compliant User Rights Management**
CATEGORY	**Control Finding**
RECOMMENDATION	We recommend OCIT develop a more robust, formal process to ensure that Managed Services vendors perform duties in accordance with the MSA regarding proper user provisioning and de-provisioning.
CURRENT STATUS	**Implemented.** Based on our review of physical access user accounts managed by Managed Services, the process of provisioning and de-provisioning access to County network resources has improved. Based on the actions taken by OCIT, we consider this recommendation implemented.

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 & PLANNED ACTION	**In Process.** OCIT advised us it has contracted a reputable cybersecurity third-party vendor to develop new IT policies, as well as revise existing policies to meet industry best practice. Management will be required to review these policies for appropriateness on an annual basis. While OCIT has finalized certain IT policies such as IT Governance and Security Patch Management, other critical IT policies were not finalized and approved. OCIT has established the Cyber Security Joint Task Force (CSJTF) to develop a uniform County IT Security Policy. The CSJTF meets monthly to review and discuss necessary changes to IT policies. Based on the actions taken by OCIT, we consider this recommendation to be in process.

AUDIT TEAM	Scott Suzuki, CPA, CIA, CISA	Assistant Director
	Jimmy Nguyen, CISA, CFE, CEH	IT Audit Manager II
	Scott Kim, CPA, CISA	IT Audit Manager I

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 follow-up audit was limited to reviewing actions taken by OCIT as of November 30, 2018 to implement the 31 recommendations from our original Audit No. 1644, dated April 10, 2018.
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.

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.