Orange County Auditor-Controller

Internal Audit

Information Technology Audit: County Executive Office/ OC Information Technology General Controls

For the Year Ended
December 31, 2016

Audit Number 1644
Report Date: April 10, 2018

ORANGE COUNTY

AUDITOR-CONTROLLER

INTERNAL AUDIT

Eric H. Woolery, CPA

Orange County Auditor-Controller

Scott Suzuki, CPA, CIA, CISA	**Director of Internal Audit**
Jimmy Nguyen, CISA, CFE	**IT Audit Manager II**
Scott Kim, CPA, CISA	**IT Audit Manager I**

12 Civic Center Plaza, Room 200
Santa Ana, CA 92701

Auditor-Controller Web Site
www.ac.ocgov.com

ERIC H. WOOLERY, CPA
AUDITOR-CONTROLLER

Transmittal Letter

Audit No. 1644

April 10, 2018

TO: Joel Golub
Chief Information Officer

SUBJECT: Information Technology Audit:
County Executive Office/OC Information Technology General Controls

We have completed our audit of the IT General Controls administered by the County Executive Office/OC Information Technology (OCIT) for the year ended December 31, 2016. Our final report is attached for your review. **Please note, due to the sensitive nature of the specific findings, details of the full report were presented to a limited audience.**

An **Audit Status Report** is submitted quarterly to the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS) detailing any critical and significant audit findings released in reports during the prior quarter and the implementation status of audit recommendations as disclosed by our Follow-Up Audits. Accordingly, the results of this audit will be included in a future status report to the AOC and BOS.

Additionally, we will request your department to complete a **Customer Survey** of Audit Services. You will receive the survey shortly after the distribution of our final report.

E Woolery

Eric Woolery, CPA
Auditor-Controller

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
Frank Kim, County Executive Officer
KC Roestenberg, Assistant CIO, CEO/OCIT
Jacob Margolis, Chief Information Security Officer, CEO/OCIT
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Macias Gini & O'Connell LLP, County External Auditor

Table of Contents

Information Technology Audit:
County Executive Office/OC Information Technology
General Controls
Audit No. 1644

For the Year Ended December 31, 2016

Table of Contents

Internal Auditor's Report

Audit No. 1644 **April 10, 2018**

TO: Joel Golub
Chief Information Officer

FROM: Eric H. Woolery, CPA
Auditor-Controller

SUBJECT: Information Technology Audit:
County Executive Office/OC Information Technology General Controls

OBJECTIVES

We have completed our audit of the IT General Controls (ITGC) administered by the County Executive Office/OC Information Technology (OCIT) for the year ended December 31, 2016. We performed this audit in accordance with the FY 2017-18 Audit Plan and Risk Assessment developed by Auditor-Controller Internal Audit Division and approved by the Audit Oversight Committee (AOC) and Board of Supervisors (BOS). Our audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors (IIA) and Control Objectives for Information and Related Technology (COBIT 5) prescribed by the Information Systems Audit and Control Association (ISACA). COBIT 5 is a business framework for the governance and management of Enterprise IT. Our audit objectives were to:

1. Ensure physical and logical security to data and programs are appropriate, approved, managed, maintained, and adequately supported.

2. Ensure change management and system development life cycle (SDLC) processes are appropriate, approved, and adequately supported.

3. Ensure computer operations are appropriately, adequately, and effectively managed to ensure timely and proper continuation of system processing.

4. Review OCIT's implementation of selected components of the IT governance model and recommend improvements.

SCOPE AND METHODOLOGY

Our audit scope was limited to general IT controls at OCIT for Managed Services and Shared Services for the year ended December 31, 2016. Our methodology included corroborative inquiry, auditor walkthrough, observation, examination, and testing of relevant supporting documentation.

Exclusions

Our audit scope did not include the following:

1. IT operations not under Managed Services or Shared Services (e.g., elected officials or departments opting to maintain separate/local IT functions).

2. Contingency planning (e.g., disaster recovery, business continuity planning). While data backup was tested and reviewed as part of ITGC operational testing, a comprehensive review and testing of OCIT disaster recovery was not performed.

3. Application controls.

4. Evaluation of OCIT performance, i.e., performance audit.

RESULTS

Objective No. 1			
We found that physical and logical security to data and programs **WAS NOT** appropriate, approved, managed, maintained, and adequately supported due to the following:	**Six (6) Critical Control Weaknesses**	Redacted	**Finding No. 1**
		Redacted	**Finding No. 2**
		Redacted	**Finding No. 3**
		Redacted	**Finding No. 4**
		Redacted	**Finding No. 5**
		Redacted	**Finding No. 6**
	Two (2) Significant Control Weaknesses	Redacted	**Finding No. 7**
		Redacted	**Finding No. 8**
	Five (5) Control Findings	Terminated access	**Finding No. 9**
		Redacted	**Finding No. 10**
		New user access	**Finding No. 11**
		Password policy	**Finding No. 12**
		Antivirus software	**Finding No. 13**
Objective No. 2			
We found that change management and SDLC processes were appropriate, approved, and adequately supported; however, we identified:	**Two (2) Significant Control Weaknesses**	Risk assessment	**Finding No. 14**
		Change management tool	**Finding No. 15**
	Four (4) Control Findings	Cloud migration strategy	**Finding No. 16**
		Emergency changes	**Finding No. 17**
		Programming standards	**Finding No. 18**
		System Development Life Cycle procedures	**Finding No. 19**
Objective No. 3			
We found that computer operations were appropriately, adequately, and effectively managed to ensure timely and proper continuation of system processing; however, we identified:	**One (1) Significant Control Weakness**	Shared services agreements	**Finding No. 20**
	Five (5) Control Findings	Redacted	**Finding No. 21**
		Backup error messages	**Finding No. 22**
		Backup schedules	**Finding No. 23**
		Incident management procedures	**Finding No. 24**
		Backup and incident management solution	**Finding No. 25**

RESULTS (CON’T)

Objective No. 4			
We found the following related to selected components of the IT governance model:	**Three (3) Significant Control Weaknesses**	Cybersecurity framework	**Finding No. 26**
		Countywide IT security authority	**Finding No. 27**
		IT risk management framework	**Finding No. 28**
	Three (3) Control Findings	Procurement documentation	**Finding No. 29**
		User rights management	**Finding No. 30**
		Policies, procedures, standards, and guidelines	**Finding No. 31**

BACKGROUND

The mission of OCIT is to provide innovative, reliable, and secure technology solutions that support County departments in the delivery of quality public services. The department was headed by an Interim Chief Information Officer (CIO) during the audit period and, as of April 2017, a full-time CIO. OCIT is comprised of eight divisions: (1) Infrastructure & Communication Services (Shared Services); (2) Managed Services Delivery (Managed Services); (3) Agency Applications; (4) Enterprise & Multi-Agency Applications; (5) Strategy, Innovation, & Architecture; (6) Customer Relationship Management; (7) Information Security; and (8) Administrative Services.

OCIT follows the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” which provides a catalog of security and privacy controls for federal information systems and organizations, and a process for selecting controls to protect organizational operations/assets, other organizations, individuals, and the nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors. A comparison between the NIST framework and the COBIT 5 framework was provided to OCIT.

Service Delivery Model

OCIT is structured in such a manner that departments can select from several service delivery options:

1. Shared Services is an in-house OCIT solution comprised of County IT personnel who support departments that do not wish to utilize the managed services model;

2. Managed Services consists of two large vendors that provide services based on managed services agreements (MSA), specifically:

   - Science Applications International Corporation (SAIC). Supports the Orange County Data Center (OCDC) facility, servers, data storage, and backup, helpdesk support, and desktop services.

- Atos (formerly Xerox State and Local Solutions, Inc.). Supports the County local area network (LAN), wide area network (WAN), network intrusion-prevention systems, web filtering, firewall, and voice over IP (VoIP) services.

Managed Services

The Managed Services model, which resulted from a need to provide County departments with cost-efficient and reliable IT services, allows for predictable costs and provides set standardized service delivery for departments. The Managed Services contracts define the service-level requirements (SLR) and associated monetary penalties in the event the vendors fail to meet the terms of the SLR. This service delivery model ensures the County receives the services it contracted and is equitably paying for the value of those services.

Managed Services Oversight

Oversight of the Managed Services contractors is performed by the Managed Services Delivery Division of OCIT. Vendors are required to produce monthly SLR reports with back-up documentation, which are reviewed and verified by the County for accuracy. This includes reconciliation of system-generated reports to those produced by the vendors. This process involves oversight of day-to-day operations as well as monthly, quarterly, and annual reviews of the service results, and fine-tuning of all applicable services and service levels to ensure that services continue to be provided in conjunction with the County's changing business needs.

Shared Services

The Shared Services initiative started in 2015, resulting from a need to provide County departments with cost-efficient, consistent, and reliable IT services. The focus of Shared Services has been to normalize service delivery through standardized hardware and software platforms, in addition to standardized processes.

Shared Services encompasses a number of IT service areas including customer relationship management, applications development and support, project management, business analysis, service desk, desktop support, and infrastructure services. Shared Services also includes information security for the following departments: OC Public Works (OCPW), OC Waste & Recycling (OCWR), OC Community Resources (OCCR), Child Support Services (CSS) and, most recently, OC Probation Department. The County is in the process of expanding the Shared Services model to other departments as it attempts to meet modern expectations with current technology, tools, and processes. Information Technology at the County has operated in a decentralized model since 1996, which has resulted in inefficient IT business process mechanisms that potentially impact reliability and services/support. The County envisions that the enhanced Shared Services model will incorporate consistent and adequate security standards, policies, and training countywide, as well as reducing operational cost through more efficient and consistent IT processes.

Prior Audit Coverage

There have been no audits with this scope at OCIT within the last ten years.

FOLLOW-UP PROCESS

Please note we have a structured and rigorous **Follow-Up Audit** process in response to recommendations and suggestions made by the AOC and the BOS. Our **First Follow-Up Audit** will generally begin at six months from the official release of the report.

A copy of all our Follow-Up Audit reports is provided to the BOS as well as to all those individuals indicated on our standard routing distribution list.

The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our **Second Follow-Up Audit** will generally begin at six months from the release of the first Follow-Up Audit report, by which time **all** audit recommendations are expected to be addressed and implemented. We bring to the AOC's attention any audit recommendations we find still not implemented or mitigated after the second Follow-Up Audit. Such open issues will appear on the AOC agenda at their next scheduled meeting for discussion.

We have attached a **Follow-Up Audit Report Form**. Your department should complete this template as our audit recommendations are implemented. When we perform our first Follow-Up Audit approximately six months from the date of this report, we will need to obtain the completed form to facilitate our review.

MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROL

In accordance with the Auditor-Controller's County Accounting Manual Section S-2 Internal Control Systems: "All County departments/agencies shall maintain effective internal control systems as an integral part of their management practices. This is because management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls." Control systems shall be continuously evaluated by Management and weaknesses, when detected, must be promptly corrected. The criteria for evaluating an entity's internal control structure is the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework. Our Internal Control Audit enhances and complements, but does not substitute for OCIT's continuing emphasis on control activities and self-assessment of control risks.

Inherent Limitations in Any System of Internal Control

Because of inherent limitations in any system of internal control, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. In addition, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in the OCIT's operating procedures, accounting practices, and compliance with County policy.

The Auditor-Controller Internal Audit Division is available to partner with your staff so that they can successfully implement or mitigate difficult audit recommendations

ACKNOWLEDGEMENT

We appreciate the courtesy extended to us by the personnel at OCIT during our audit. If you have any questions regarding our audit, please contact me at (714) 834-2456, or Scott Suzuki, Director of Internal Audit, at (714) 834-5509.

Detailed Findings, Recommendations, and Management Responses

IT Process and Internal Control Strengths

Process and internal control strengths noted during our audit include:

- ✓ The Chief Information Officer position was filled.
- ✓ The Cyber Security Team has been recently staffed, and responsibility for performing a cyber-resilience assessment has been assigned.
- ✓ Progress of County IT projects is reported quarterly to the Board of Supervisors (BOS).
- ✓ Managed Services performs customer surveys on helpdesk ticket support provided, which is a measure of performance against the service-level agreements and service-level requirements.
- ✓ Managed Services performs a thorough and extensive review of the service-level requirements for the Managed Services vendor Atos.
- ✓ Although there were no formal service-level agreements or requirements for Shared Services, Shared Services responded to incident requests timely.
- ✓ Proper environmental controls over the OC Data Center (OCDC) server room areas.
- ✓ Each employee badge swipe allows a single employee entry; piggybacking is not permitted.
- ✓ Visitors must sign in with front desk personnel and visitors are appropriately escorted upon entry of server room areas.

The following areas are where IT processes and internal control should be enhanced:

Objective 1: Ensure physical and logical security to data and programs are appropriate, approved, managed, maintained, and adequately supported.

Finding Nos. 1, 2, 3, 4, 5, 6, 7, 8 and 10 were removed from this report version due to the sensitive nature of the specific findings. OCIT management concurred with each of the associated recommendations.

Finding No. 9 – Terminated Access Not Properly Documented (Control Finding)

We found that supporting documentation to evidence that IT was appropriately notified of employee termination, prior to disabling network-user access, for Shared Services was not available.

A high rate of terminated users with rights-granting access to the County network, firewall, and data significantly heightens cybersecurity risk.

Lack of documentation of employee termination indicates that the process to terminate or de-provision user access rights on the network significantly increases the risk of unauthorized access to County data.

We sampled 25 terminated users across three entities: Managed Services, Shared Services, and County vendors (SAIC and Atos). We found eight of the 25 (28%) samples lacked the proper documentation to request the removal of network user access for terminated employees. Of the eight users, Atos was unable to provide documentation for five terminated users. The following was noted:

- Three of 25 (12%) Shared Services users had terminated with no documentation supporting their removal.

- One of 25 (4%) Atos users had an administrative account that should have been terminated but was still active in Active Directory.

- OCPROFILE, an in-house application that contains listings of Managed Services contractor's employee activities, was not being properly updated by Atos.

- One of 25 (4%) County employees managed by SAIC had terminated in November 2016 but had a network account on the CEOIT domain.

As a result of our audit fieldwork, we were informed that OCIT will be working with the vendors to amend the contracts with both SAIC and Atos to add a Service Level Requirement that financially penalizes them if the employment status data is not updated properly and timely. In addition, departments also have the responsibility to notify OCIT of terminations and changes in employment. OCIT is unable to effect this change on its own, as it will need collaboration with all departments.

Recommendation No. 9
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

Recommendation 1: OCIT has had an operational best practice in place since 2016 which requires all staff be entered into [redacted] (our active employee tracking system).

This system keeps track of both County staff and Contractors. The identified issue was that contract vendors in some cases were not providing updates consistently on a timely basis. Atos has confirmed that they understand the gravity of ensuring that the accurate and timely reporting of this information is critical to County security. To help ensure that timely updates are provided going forward, OCIT is amending the Atos contract to add a Service Level Requirement that financially penalizes Atos if the employment status data is not properly up to date. The amendment will be in place on or before March 2018.

OCIT will provide refresh training on [redacted] by March 2018, and also offer on-demand and annual training as staffing requires. Training will also be provided to all new hires within 90 days of their hire date. In addition, OCIT will perform audits every 60 days of user accounts that have not successfully logged into the network within the past 30 days. Any account that meets these criteria will immediately be disabled. This recommendation has been implemented as of August 2017.

Recommendation 2: OCIT has a service desk managed Onboarding/Off-Boarding Process in place. This process generates a ticket and assigns the request to delete network access when a staff member leaves. We are in the process of adopting [redacted] (SMS) as our service management tool. We will have SMS implemented by September 2018.

Recommendation 3: OCIT is currently reviewing this recommendation and will determine the feasibility of setting expiration dates for contractor logical access by June 2018.

Finding No. 11 – New User Access Lacked Management Approval (Control Finding)

New users were granted access to IT resources without required approvals.

Undocumented approvals granting access to the County network, given the heightened risks associated with cybersecurity, significantly introduces the risk of unauthorized access to County sensitive data.

We sampled new user network access across three entities: Managed Services, Shared Services and County vendors (SAIC and Atos). We found seven of 25 (28%) lacked proper new user access approvals to the network. Of the seven users, two new user access requests lacked supporting documentation showing evidence of management’s approval. Additionally, for the remaining five users identified, Atos was unable to provide documentation because we were unable to identify a population of users for testing.

Recommendation No. 11:
We recommend OCIT ensure requests for new user access to network resources are appropriately authorized by management and documented prior to provisioning access.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT has a service desk managed Onboarding/Off-Boarding Process in place. This process generates a ticket and assigns the request to the Data Center Facility team to issue or delete network access for new employees.

This process is also used to generate a ticket to the Data Center Facilities team to deactivate access when a staff member leaves. OCIT will modify the process by June 2018 to ensure employee network access is authorized by the requestor's supervisor or authorized delegate.

Finding No. 12 – Countywide IT Security Policy Does Not Address Certain Password Security Settings (Control Finding)

We found the current Countywide IT Security Policy does not address and/or enforce password settings for password history (reuse of previous passwords) and lockout threshold (invalid login attempts before user is locked out).

Lack of sufficient password configuration rules could result in an unauthorized user easily gaining access to the network, e.g., via brute force attack. User account password settings should be enhanced to prevent unauthorized access.

Recommendation No. 12:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

In March 2017, OCIT implemented the use of complex passwords.

Recommendation 1: OCIT has contracted a vendor to develop OCIT Security policies that address robust password configuration settings. The policies will include a requirement that the policy be reviewed at least annually and will address a more robust password configuration management policy. The policies will be presented to the Board of Supervisors for approval by June 2018.

Recommendation 2: OCIT will review password configuration rules annually to adhere to the County IT Security policy.

Finding No. 13 – Current Antivirus Software Not Installed on System Component (Control Finding)

One Windows Server did not have the most current antivirus/malware software and definitions installed as recommended by the vendor.

A lack of current antivirus software definitions can result in an introduction to viruses and malware attacks (which perform malicious acts, such as deleting files and accessing personal data).

Deployment of current antivirus and malware definitions are controlled by an antivirus management console, which is designed to automatically deploy and install the most current definitions to servers and workstations as recommended by the vendor for Managed Services and Shared Services.

We reviewed system components from three entities: Managed Services, Shared Services, and County vendors (SAIC and Atos). The review encompassed over 7,000 devices and found the aforementioned single Windows Server did not have the most current antivirus/malware software and definitions installed as recommended by the vendor for Shared Services. This particular server resides at the [redacted] Disaster Recovery site and does not have Internet access or access to the County management server, which reduces the risk of a virus and malware infection to the County computer network. While the Windows Server does not have Internet access, it is connected to the County Wide Area Network (WAN) which means that in the event a virus is introduced to the network, it could significantly impact the Disaster Recovery Windows Server. Shared Services management agrees the server should be installed with the current security updates as recommended by the vendor.

As a result of our audit fieldwork, OCIT notified us the Windows Server had been updated to include the most current antivirus/malware software and definitions.

Recommendation No. 13:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT's best practices requires that all servers and desktops under our management responsibility, to be patched with the most current Antivirus software on a regular basis. The vast majority of these devices are properly patched. We also prudently apply security patches on an ad hoc basis as known vulnerabilities occur. The previously missed device has now been added to our Configuration Management Data Base, CMDB. The identified device should have been maintained by our vendor. This will ensure that all devices, County and those owned by our managed services vendors, are properly patched. OCIT will review the CMDB quarterly to ensure all devices are properly patched. This process will be implemented starting July 2018.

In July 2017, OCIT completed its deployment of a centrally managed antivirus software. The implementation standardized protection settings for all servers, including ones that were not previously under central management (under its purview).

Objective 2: Ensure change management and system development life cycle (SDLC) processes are appropriate, approved, and adequately supported.

Finding No. 14 – Change Request Risk Assessment Not Consistently Completed (Significant Control Weakness)

A risk assessment is not consistently completed for normal change requests performed by Managed Services.

Lack of a risk assessment could result in budget overruns, schedule slips, wrong functionality, and issues with interface, performance, reliability, and availability.

We sampled normal change requests performed by Managed Services and their vendors, SAIC and Atos. Out of the 20 normal change requests sampled, 14 (70%) did not have a risk assessment performed and included in the change ticket. Per discussion with OCIT and SAIC, there was no practice for a risk assessment to be completed and submitted with a change request, despite documented change-management procedures requiring a risk assessment be completed.

As a result of our finding and discussion with Managed Services management, effective immediately, the change manager will not approve a change request submitted without a completed risk assessment. Furthermore, OCIT is working on programming the change-management monitoring tool to reject a change request if a completed risk assessment is not included.

Recommendation No. 14:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

As of November 2017 OCIT requires all change requests to be submitted with a detailed risk assessment. During the weekly Change Advisory Board meeting, participants review all change requests and if a risk assessment is not provided the request is denied.

Finding No. 15 – Shared Services Change Management Tool Lacked Critical Information (Significant Control Weakness)

During a walkthrough of the Shared Services Change Management Tool, which uses a SharePoint portal, we noted that it lacked critical change information such as the status (open, in process, closed), timestamps, Change Advisory Board (CAB) meeting date of when the change request was reviewed and approved, and CAB Chair review, approval sign-offs, and dates.

Changes that do not indicate evidence of critical elements to perform system changes create a risk that changes may be introduced and migrated to production in an unstructured and unapproved manner, which could result in unauthorized modifications being performed.

As a result of our finding and discussion with Shared Services management, management informed us there are long-term plans to utilize a different change-management tool but, in the interim, SharePoint would be modified to include critical information.

Recommendation No. 15:
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.

OCIT Management Response:
Concur. OCIT agrees with the finding.

As of June 2017, OCIT made short term changes to our processes per the above recommendations. We are in the process of adopting [redacted] (SMS) as our change management tool. We will have SMS implemented by September 2018.

Finding No. 16 – Application Cloud Migration Strategy Not Finalized (Control Finding)

OCIT has not finalized its Application Cloud Migration Strategy.

Lack of a comprehensive and finalized plan to migrate applications to the Cloud can introduce inadequate programming standards, insufficient details of migration approach from on premise to off premise, inconclusive testing results, and possibly introduce security vulnerabilities in the cloud solution. Furthermore, changes to the process could be introduced after the draft has been issued. These undocumented changes may not be approved or properly incorporated into future migration strategy.

OCIT's Application Cloud Migration Strategy for Microsoft Azure documents OCIT's procedures for migration of applications into the cloud network. This document is in draft status as a finalized copy was not available to review.

Based upon review of the draft copy, there were some concerns identified regarding OCIT's first migration of an application into a cloud network that were not addressed in the draft copy. Of note, there was a lack of procedures for ensuring documentation and information relating to issues that arose from user acceptance testing is maintained. This includes information such as identification of cause of the issue, what was done to resolve the issue, who performed the resolution, and authorized changes to be migrated into production.

Recommendation No. 16:
We recommend OCIT finalize the Application Cloud Migration Strategy and ensure appropriate documentation is created and maintained for all application migrations into the Cloud.

OCIT Management Response:
Concur. OCIT agrees with the finding.

OCIT continues to update the document and will have the strategy finalized by March 2018. All application migrations have and will be conducted in accordance with OCIT Project Management practices, methodologies and documentation requirements.

Finding No. 17 – Emergency Changes Were Not Reviewed After Implementation (Control Finding)

Emergency changes completed by Managed Services and their vendors, SAIC and Atos, were not reviewed after implementation by the Change Advisory Board (CAB).

Emergency changes that do not follow the defined change-management procedures could result in emergency changes being introduced into production that are unauthorized or changes not working as expected. Furthermore, there is an increased potential to miss opportunities for process improvement and evaluations for better results in future changes.

We reviewed emergency changes completed by Managed Services and their vendors, SAIC and Atos. Six of 15 (40%) changes reviewed were not included in any CAB meeting minutes. Documented change-management procedures require an emergency change request be reviewed by CAB post-implementation.

As a result of our finding and discussion with Managed Services management, the weekly CAB agenda will include emergency changes that were not previously reviewed.

Recommendation No. 17:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

As of May 2017, OCIT has amended its procedures to ensure that all emergency changes, not discussed in the previous CAB, are reviewed during the next scheduled CAB meeting.

Finding No. 18 – Programming Standards Not Documented (Control Finding)

OCIT does not have a current programming standards document.

Lack of defined programming standards can result in inconsistencies in coding style. Differences in paragraphs, indentation, naming conventions, functions, and commenting can result in difficulty in deciphering what programmers have written and developed in program code.

During our interviews, we requested documentation reflecting OCIT's programming standards. Coding standards are intended to facilitate consistencies in naming conventions and ease in maintenance of program code. Coding standard provides a guideline for how developers write code to the standards outlined in the document, ensuring consistency in the coding style.

OCIT provided an outdated standard that was written specifically for one of the Shared Services departments. Programming standards should be up-to-date and adhered to for changes of in-scope application(s) prior to migration into production.

Recommendation No. 18:
We recommend OCIT develop and formalize a documented programming standard that is consistent across all applications.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT is currently reviewing this recommendation and will determine the feasibility of developing and formalizing a documented programming standard that is consistent across all applications by June 2018.

Finding No. 19 – System Development Life Cycle Procedures Not Documented (Control Finding)

There are no up-to-date documented system development life cycle (SDLC) procedures.

Lack of documented SDLC procedures can result in systems being developed that are not in line with best practices, systems not meeting all the customer needs, and systems not being developed to meet all the technical specifications.

A documented SDLC was provided for a specific application and was noted as the framework for the other OCIT enterprise applications but does not reflect some of the current SDLC tools utilized by OCIT such as [redacted] and Application Portfolio Management.

With the digital transformation initiatives that are ongoing, it is critical that properly documented SDLC procedures are created to provide guidance, especially, as software is now being built to access the Cloud.

Recommendation No. 19:
We recommend OCIT update their written SDLC 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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT Development continues to follow the standard Software Development Lifecycle Process (SDLC), both Waterfall and Agile Methodologies. These methodologies are identified in the OCIT Project Management Framework document. OCIT Development has selected and implemented [redacted] as the primary tool to manage SDLC. OCIT Development has also created an Application Portfolio Management Tool to assist in tracking the Application Life Cycle. OCIT Development updated the SDLC document to reflect this newly developed tool and usage of [redacted] in September 2017.

Objective 3: Ensure computer operations are appropriately, adequately, and effectively managed to ensure timely and proper continuation of system processing.

Finding No. 21 was removed from this report version due to the sensitive nature of the specific finding. OCIT management concurred with the associated recommendation.

Finding No. 20 – Shared Services Lacks Service Level Agreements/Requirements with Client Departments (Significant Control Weakness)

While we found Service Level Agreements (SLA) and Service Level Requirements (SLR) in the Master Service Agreement (MSA) with SAIC and Atos, Shared Services does not have any SLAs and SLRs with departments they serve.

SLAs and SLRs serve as a performance measure of success in achieving agreed upon and expected service outcomes by OCIT, the service provider. The criteria measures success rate to-date, assists management in identifying factors impacting achievement of success criteria, and serves as a method to enhance processes to improve performance measures.

The absence of SLAs and SLRs can result in Shared Services not adequately meeting the customer's expectations. Although Shared Services utilizes satisfaction surveys and customer focus groups, these do not provide clearly measurable key performance indicators and benchmarking of the services provided. This could result in inefficiencies and loss of resources by departments under the Shared Services model.

Recommendation No. 20:
We recommend OCIT Shared Services develop standardized SLAs and/or SLRs for services provided across all Shared Services departments to enable monitoring of performance.

OCIT Management Response:
Concur. OCIT agrees with the finding.

As of June 2017, OCIT made immediate changes to our processes per the above recommendations. By September 2018, OCIT will merge all ticketing systems with the centrally managed [redacted] instance, at which time OCIT will identify and manage Service Level Requirements.

Finding No. 22 – Error Messages Not Configured For Abended Backup Jobs (Control Finding)

The Child Support Services (CSS) backup tool did not have enabled error message notifications for the computer operator when a scheduled backup job did not complete or ended abnormally (abended).

Timely notification of error messages during backup jobs is critical to ensure backup jobs that abended are detected, re-run timely, and retained in the event of system failure or data loss.

Furthermore, a lack of error messages in backup jobs could result in CSS data being completely lost or the inability to restore data in the event of a system outage or disaster.

We reviewed three versions of Veritas (formerly Symantec) Backup Exec (utilized across Shared Services departments OCCR, OCWR, and CSS) to determine whether error messages were generated for incomplete jobs. Only the exception at CSS was noted.

As a result of our finding, Shared Services Management acknowledged error messages were disabled and immediately enabled error messages to notify computer operators of abended backup jobs.

Recommendation No. 22:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT enabled and verified the notifications on all backup jobs in May 2017. OCIT will periodically review backup tools configuration to notify staff of any backup job failure.

Finding No. 23 – Backup Jobs Schedule Not Current (Control Finding)

Shared Services systems showed multiple backup jobs that failed and were not re-run. Upon inquiry, it was noted these jobs were obsolete.

Backup jobs that fail on the backup job schedule can go undetected by personnel resulting in data being completely lost. Additionally, there may be inefficiencies due to loss of time from researching abended jobs that are obsolete and computing resources may be expended on unnecessary jobs.

We reviewed three versions of Veritas (formerly Symantec) Backup Exec (utilized across Shared Services departments OCCR, OCWR, and CSS). There were several backup jobs reviewed across the three instances of Backup Exec that abended and were not re-run. Management indicated there were obsolete jobs on the schedule that needed to be removed, as they no longer required those jobs to be run by the scheduler. Per discussion with OCIT staff, there were no formal procedures for periodically reviewing and updating scheduled jobs, which resulted in obsolete jobs abending.

Since management did not provide formal documentation supporting jobs that were no longer required, it was not apparent how personnel could distinguish obsolete jobs from current jobs within the tool.

As a result of our finding and discussion with Shared Services Management, an "IT Standard – Backup & Restore Guideline" procedure was created that included a process for quarterly review of scheduled backup jobs, and review by the Shared Services team for changes.

Recommendation No. 23:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT reviewed the backup jobs in May 2017, and removed any unnecessary and duplicate jobs. Shared Services staff will review all backup jobs bi-annually to ensure they are current.

Finding No. 24 – Escalation Procedures for Incident Management Not Documented (Control Finding)

Although the Shared Services team met daily and performed a review of outstanding incidents and authorization for incidents, a formal escalation procedure was not documented to specify measures to be implemented at times where prompt attention is required for an incident that may severely impact business and operations.

A lack of formal escalation procedures can result in incidents not being addressed in a timely manner, downtime, or inability to perform work.

As a result of our finding and discussion with Shared Services management, management created the “IT Standard – Help Desk – Incident Escalation Process” that documents escalation procedures. They further noted the procedure would be updated once Shared Services had consolidated incident management tools into one platform.

Recommendation No. 24:
We recommend OCIT implement and follow its escalation procedures, and update the procedures for any significant changes.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT holds bi-weekly ticket review meetings to address all necessary ticket escalation. Managed Services has been holding meetings since the inception of the contract March 2014. Shared Services is in the process of adopting [redacted] (SMS) as our service management tool to implement escalation procedures. We will have SMS implemented by September 2018.

Finding No. 25 – Redundant Backup and Incident Management Solutions (Control Finding)

Shared Services utilizes four different backup solutions and three incident management tools.

Multiple tools, solutions, and personnel performing the exact same processes for backups and incident management can result in inefficient and ineffective use of County resources.

Four different backup solutions and three incident management tools are used for OCCR, OCWR, CSS, and OCPW. OCIT staff are assigned to schedule, authorize, perform, and review backup jobs performed by each different version and tool. In addition, there were different personnel managing the various tools and solutions to perform the same processes.

OCIT informed us that Shared Services management identified the redundant nature of the current backup and incident management solution was due to a lack of time to consolidate. Management had already recognized the importance of decreasing redundancies and had made plans to consolidate activities and process tools to gain efficiencies by migrating Shared Services incident management tools onto one solution. Furthermore, Shared Services is currently in the process of integrating an Enterprise backup solution.

Recommendation No. 25:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT is working with the Strategy and Architecture group on an enterprise backup solution. OCIT is also looking into implementing [redacted] Incident Management Solution for all the Shared Services agencies. OCIT will adopt both a centralized backup and incident management solution by September 2018.

Objective 4: Review OCIT's implementation of selected components of the IT governance model and recommend improvements.

Finding No. 26 – Cybersecurity Framework Not Fully Implemented (Significant Control Weakness)

While a cybersecurity framework is in the design phase, it has not been fully designed, implemented, and deployed.

A cybersecurity framework that has not been fully implemented can result in County resources being inadequately protected. If a framework inclusive of training, knowledge, and documentation were in place, the County would be in an optimal position to resolve security events such as denial of service attacks, system breaches, virus attacks, ransomware attacks, unauthorized access to data, loss of information, system outages, and reputational damage to the County.

OCIT has made progress toward establishing a cybersecurity framework including developing a mission statement, hiring a team of security personnel, performing cybersecurity awareness training, creating a road map for the framework, and commencing cybersecurity initiatives. One of the important elements is a cybersecurity program has been developed, but the rollout and deployment of that program has yet to be performed.

During our audit, we were informed that at the end of 2016, the BOS approved the current IT Governance structure. Under this structure, the Chief Information Security Officer (CISO) has oversight over the County Cyber Security Program, and County IT policies are reviewed and approved by the IT Executive Council. The Cyber Security Joint Task Force was formed under the IT Executive Council and tasked with developing the Cyber Security Manual by April 2018, which incorporates the Countywide IT security requirements. Once completed, the Cyber Security Manual will be reviewed and approved by CEO and the IT Executive Council for implementation. The manual and security program are based on the Department of Homeland Security Cyber Resilience Review and National Institute of Standards and Technology (NIST) SP800-53 Rev. 4. The Task Force approved the security program requirements at its July 2017 meeting.

In addition, OCIT started developing the requirements for a Request for Proposal (RFP) to obtain cybersecurity assessment services. The RFP was released in November 2016, and the contract awarded in April 2017.

Recommendation No. 26:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT has established the Cybersecurity Joint Task Force to develop minimum requirements for departments to create their own cybersecurity programs. These minimum requirements will be documented in a County Cybersecurity Manual establishing a common set of standards and practices to improve and enhance the cyber security posture for all County departments. The cybersecurity program requirements are based on Department of Homeland Security Cyber Resilience Review (CRR) which uses the Cyber Resilience Evaluation Method and the CERT® Resilience Management Model (CERT-RMM), both developed at Carnegie Mellon University's Software Engineering Institute. The CRR cross references with the NIST Cybersecurity Framework – Identify, Protect, Detect, Respond, Recover. The Cybersecurity Manual addresses such topics 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, etc.)
- Operational Controls (processes to implement policies)
- County Plans (Incident Response, Business Continuity, Disaster Recover, Risk Management)

Cyber Security Framework addresses such topics as:

- Asset Management
- Change and Configuration Management
- Controls Management
- Incident Management
- Vulnerability Management

- Risk Management
- Service Continuity Management
- External Dependency Management
- Training and Awareness
- Situational Awareness

The Cybersecurity Manual is expected to be completed by April 2018. Once completed, the Cybersecurity Manual will be reviewed and approved by Board-approved IT governance model.

Finding No. 27 – Security Risks From Lack of Countywide IT Security Authority (Significant Control Weakness)

The OCIT executive management team does not believe they have the authority or influence to propose IT security policy with departments under the CEO.

Without countywide IT security authority, uniform IT security standards cannot be enforced by a single entity to reduce the risk of a security breach.

While each department is considered autonomous, a security breach in one department can impact the County's network as a whole, due to the interconnectivity of the County's enterprise network.

We found that the Board of Supervisors approved the current IT Governance structure at the end of 2016, where the Chief Information Security Officer (CISO) has oversight over County Cyber Security Program and County IT policies are reviewed and approved by the IT Executive Council. The Cyber Security Joint Task Force is also a committee formed under the IT Executive Council and is tasked with developing the Cyber Security Manual by April 2018, which incorporates the Countywide IT security requirements. Once completed, the Cyber Security Manual will be reviewed and approved by CEO and IT Technology Council for implementation.

Recommendation No. 27:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT is preparing an Agenda Staff Report (ASR) for the Board to approve the centralization of information security under OCIT. The ASR is expected to be presented to the Board of Supervisors in June 2018.

Finding No. 28 – Lack of Comprehensive IT Risk Management Framework (Significant Control Weakness)

A comprehensive IT risk management framework has not been adopted by OCIT.

Inadequate risk management can result in: (1) a failure to identify material risk or low probability risk with catastrophic impact, (2) excessive costs due to focusing IT resources on mitigating less strategic risk, (3) business exposure to losses due to unidentified or improperly classified risk, (4) identified risk not remediated due to lack of follow-up and/or lack of monitoring of mitigation projects, (5) misaligned risk efforts due to use of differing metrics for probability, (6) cost impacts to different business groups, or (7) unavailable business functions or processes dependent on IT.

A comprehensive IT risk management framework has not been designed, developed, and implemented to monitor and report issues. IT policies, standards, and procedures that exist are significantly dated. An IT risk management framework includes, but is not limited to, risk strategy (owners, stakeholders, communication strategy, frequency of monitoring), risk register (vendor management, software licenses, configuration management), risk mitigation plan (accept, avoid, insure), risk type, risk domain, and remaining/residual risk.

OCIT management has taken steps to implement a Governance, Risk, and Compliance (GRC) solution that will formalize IT risk management, with a target implementation date in November 2017. Ad hoc risk management processes are already in-place for the change management, project management, and disaster recovery processes.

Lastly, the risk-management processes are being matured to comply with the NIST risk management framework.

Recommendation No. 28:
We recommend OCIT continue to develop a comprehensive IT risk management framework that incorporates all risk areas including areas outside cybersecurity.

OCIT Management Response:

Concur. OCIT agrees with this finding.

OCIT has established the Cybersecurity Joint Task Force to develop minimum requirements for departments to create their own cyber security programs. These minimum requirements will be documented in a County Cybersecurity Manual establishing a common set of standards and practices to improve and enhance the cyber security posture for all County departments.

The cybersecurity program requirements are based on Department of Homeland Security Cyber Resilience Review (CRR), which uses the Cyber Resilience Evaluation Method and the CERT® Resilience Management Model (CERT-RMM), both developed at Carnegie Mellon University's Software Engineering Institute. The CRR cross-references with the NIST Cybersecurity Framework – Identify, Protect, Detect, Respond, Recover. The Cybersecurity Manual will address IT risk management and establishes the following requirements:

- A strategy for identifying, analyzing, and mitigating risks is developed
- Risk tolerances are identified
- Risks are identified
- Risks are analyzed and assigned a disposition
- Risks to assets and services are mitigated and controlled

The Cybersecurity Manual is expected to be completed by April 2018. Once completed, the Cybersecurity Manual will be reviewed and approved by Board-approved IT governance model.

In addition, risk management is on OCIT's cyber security strategic roadmap. OCIT is in the process of implementing a GRC platform, which will provide risk management capabilities to the departments countywide by July 2018.

Finding No. 29 – Incomplete Application Procurement Documentation (Control Finding)

Complete documentation for the procurement of a Cloud solution was not available.

Documentation available for the procurement of Microsoft Azure did not demonstrate adherence to the Countywide Information Technology Governance Strategy and was not consistent with the governance principles of accountability and transparency (e.g., documenting analysis and rationale for key decisions, who was involved with key decisions).

Specifically, the following steps required by the Countywide Information Technology Governance Strategy were not documented:

- The business case for the Cloud to ensure it fulfills both the IT Investment Review Board and the IT Executive Council requirements for a Cloud implementation, including gaining operational and financial benefits.

- An assessment of Cloud solution providers (e.g., Google, Amazon Web Services, IBM Cloud, or Microsoft Azure) to determine the best fit for the County based upon evaluation of County and business requirements.

Recommendation No. 29:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

As of September 2017, key OCIT managed projects go through the OCIT Intake process, in which OCIT management reviews, prioritizes, and assigns a project lead or project manager to provide project management oversight and ensure the appropriate project documentation is produced.

Finding No. 30 – Non-Compliant User Rights Management (Control Finding)

We noted that Managed Services vendors performed activities that were believed to be consistent with the fulfilment of the Managed Services Agreement (MSA); however, we found the following:

- De-provisioning of users' access rights (logical and physical) who had departed from the County, specifically pertaining to SAIC and Atos, was inconsistent.
- Provisioning of users' access rights (logical and physical) did not adhere to County policy of retaining records of access granted.
- Certification of users' access rights was not performed on a periodic basis.

Inadequate provisioning and de-provisioning of user access rights could result in unauthorized access to County data via logical or physical platforms, software license compliance issues, or unauthorized physical access to network and computer operations.

Some of these critical user access rights granted former Atos employees access to the County network infrastructure and SAIC employees who access to the computer operations, which are essentially the highest rights granted to users (e.g., access to critical County network data, OCIT facilities, desktop support, server support, network and network devices support, exchange support, VOIP support, and applications).

Recommendation No. 30:
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.

OCIT Management Response:

Concur. OCIT agrees with this finding.

OCIT contracts with SAIC and Atos to provide IT "Services" in many cases the County does not own or operate the equipment (e.g. firewalls, network devices such as routers, switches etc.). Access to vendor owned and operated systems and equipment is prohibited by Atos and SAIC and only Atos and SAIC employees have access to their respective systems and equipment. In order to address this issue with our contracted vendors OCIT has had an operational best practice in place since 2016 which requires all staff be entered into [redacted] (our active employee tracking system). This system keeps track of both County staff and Contractors. The identified issue was that contract vendors in some cases were not providing updates consistently on a timely basis. Our contractors understand the gravity of ensuring that the accurate and timely reporting of this information is critical to County security. As such they have significantly improved their processes for updating the information promptly.

To help ensure that timely updates are provided going forward OCIT is amending our contracts with both SAIC (amended January 2018) and Atos to add a Service Level Requirement that financially penalizes our vendors if the employment status data is not properly up to date. The amendment will be in place for Atos on or before March 2018.

Finding No. 31 – County IT Policy, Procedures, Standards, and Guidelines Are Outdated (Control Finding)

County IT policies, procedures, standards, and guidelines were outdated.

Inadequate policies, standards, guidelines, and procedures can result in a lack of understanding, delayed implementation of systems, security violations, and deployment of various IT systems, which could compromise countywide assets.

The policies, procedures, standards, and guidelines for the County were provided from various sources including SAIC, Atos, and the intranet for OCIT. We received numerous policies and procedures that were dated from 2004 to 2014. There was no clear evidence that a formal management oversight and monitoring process occurred to ensure the policies, procedures, standards, and guidelines were current. We reviewed the following documents and noted they were outdated:

Table 1. County IT Policies, Procedures, Standards, and Guidelines

Document	Release Date
IT Usage Policy	1/08/2010
User Provisioning Policy	7/26/2011
Patch Management	01/28/2004
IT Governance	2014
IT Security Policy	2009

Source: OCIT

As a result of our audit fieldwork, OCIT advised us the County had a County Policy Formatting Guide in place as of June 2016. In addition, a County Policy Flowchart was created for County departments to follow when determining which department has ownership of a policy and for ensuring the policy is periodically maintained and reviewed.

Recommendation No. 31:
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.

OCIT Management Response:
Concur. OCIT agrees with this finding.

OCIT has contracted a vendor to develop OCIT Security policies, and the policies will include a requirement to be reviewed at least annually, thereafter. The policies will be presented to the Board of Supervisors for approval by June 2018.

In line with OCIT's operational best practice and our master service agreements with both Atos and SAIC require that Atos and SAIC update all of their standard operating procedures as needed to properly provided the services OCIT contracts for. OCIT reviews all SOP procedures with the vendor on an annual basis to verify that old, new, and existing SOP's are in place and current. The next annual review and update will be completed March 2018.

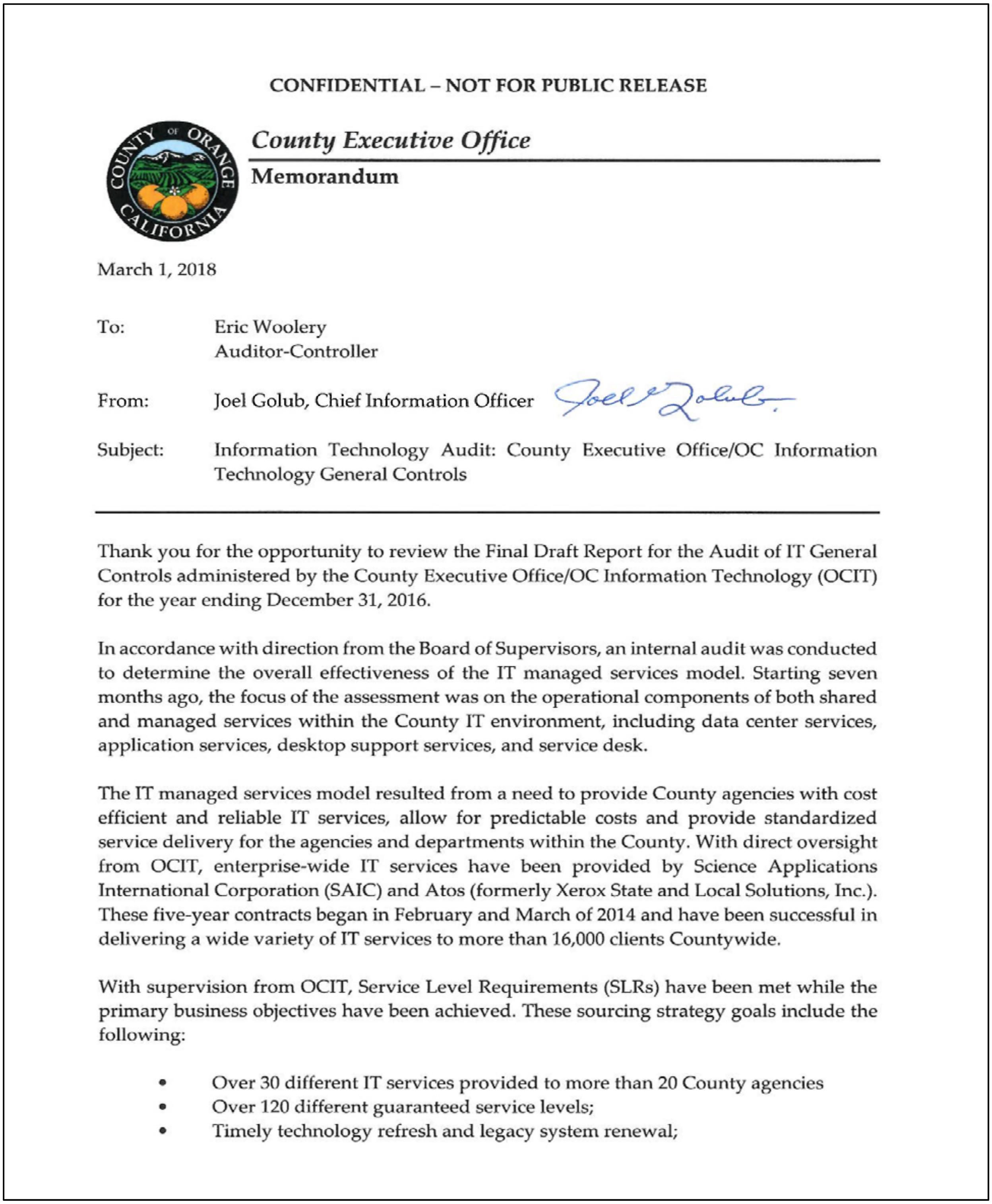
OCIT will review and update the process for maintaining IT policies by December 2018.

ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit findings and recommendations, we will classify audit report items into three distinct categories:

Critical Control Weaknesses	Significant Control Weaknesses	Control Findings
These are audit findings or a combination of audit findings that represent critical exceptions to the audit objective(s) and/or business goals. Such conditions may involve either actual or potential large dollar errors or be of such a nature as to compromise the department's or County's reputation for integrity. Management is expected to address **Critical Control Weaknesses** brought to its attention immediately.	These are audit findings or a combination of audit findings that represent a significant deficiency in the design or operation of internal controls. **Significant Control Weaknesses** require prompt corrective actions.	These are audit findings concerning internal controls, compliance issues, or efficiency/effectiveness issues that require management's corrective action to implement or enhance processes and internal controls. **Control Findings** are expected to be addressed within our follow-up process of six months, but no later than twelve months.

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses



CONFIDENTIAL – NOT FOR PUBLIC RELEASE

County Executive Office

Memorandum

March 1, 2018

To: Eric Woolery
Auditor-Controller

From: Joel Golub, Chief Information Officer Joel Golub

Subject: Information Technology Audit: County Executive Office/OC Information Technology General Controls

Thank you for the opportunity to review the Final Draft Report for the Audit of IT General Controls administered by the County Executive Office/OC Information Technology (OCIT) for the year ending December 31, 2016.

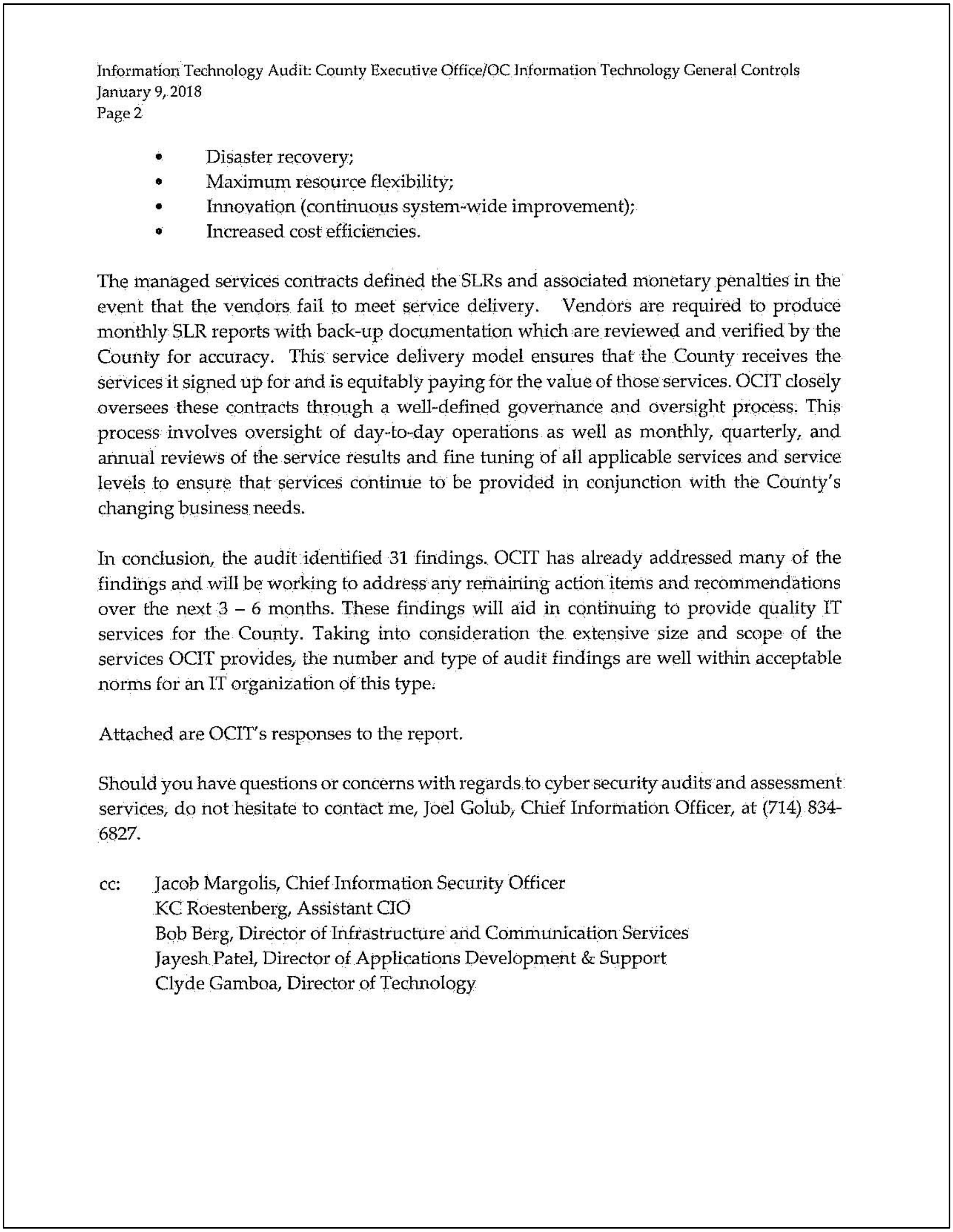
In accordance with direction from the Board of Supervisors, an internal audit was conducted to determine the overall effectiveness of the IT managed services model. Starting seven months ago, the focus of the assessment was on the operational components of both shared and managed services within the County IT environment, including data center services, application services, desktop support services, and service desk.

The IT managed services model resulted from a need to provide County agencies with cost efficient and reliable IT services, allow for predictable costs and provide standardized service delivery for the agencies and departments within the County. With direct oversight from OCIT, enterprise-wide IT services have been provided by Science Applications International Corporation (SAIC) and Atos (formerly Xerox State and Local Solutions, Inc.). These five-year contracts began in February and March of 2014 and have been successful in delivering a wide variety of IT services to more than 16,000 clients Countywide.

With supervision from OCIT, Service Level Requirements (SLRs) have been met while the primary business objectives have been achieved. These sourcing strategy goals include the following:

- Over 30 different IT services provided to more than 20 County agencies
- Over 120 different guaranteed service levels;
- Timely technology refresh and legacy system renewal;

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



Information Technology Audit: County Executive Office/OC Information Technology General Controls
January 9, 2018
Page 2

- Disaster recovery;
- Maximum resource flexibility;
- Innovation (continuous system-wide improvement);
- Increased cost efficiencies.

The managed services contracts defined the SLRs and associated monetary penalties in the event that the vendors fail to meet service delivery. Vendors are required to produce monthly SLR reports with back-up documentation which are reviewed and verified by the County for accuracy. This service delivery model ensures that the County receives the services it signed up for and is equitably paying for the value of those services. OCIT closely oversees these contracts through a well-defined governance and oversight process. This process involves oversight of day-to-day operations as well as monthly, quarterly, and annual reviews of the service results and fine tuning of all applicable services and service levels to ensure that services continue to be provided in conjunction with the County's changing business needs.

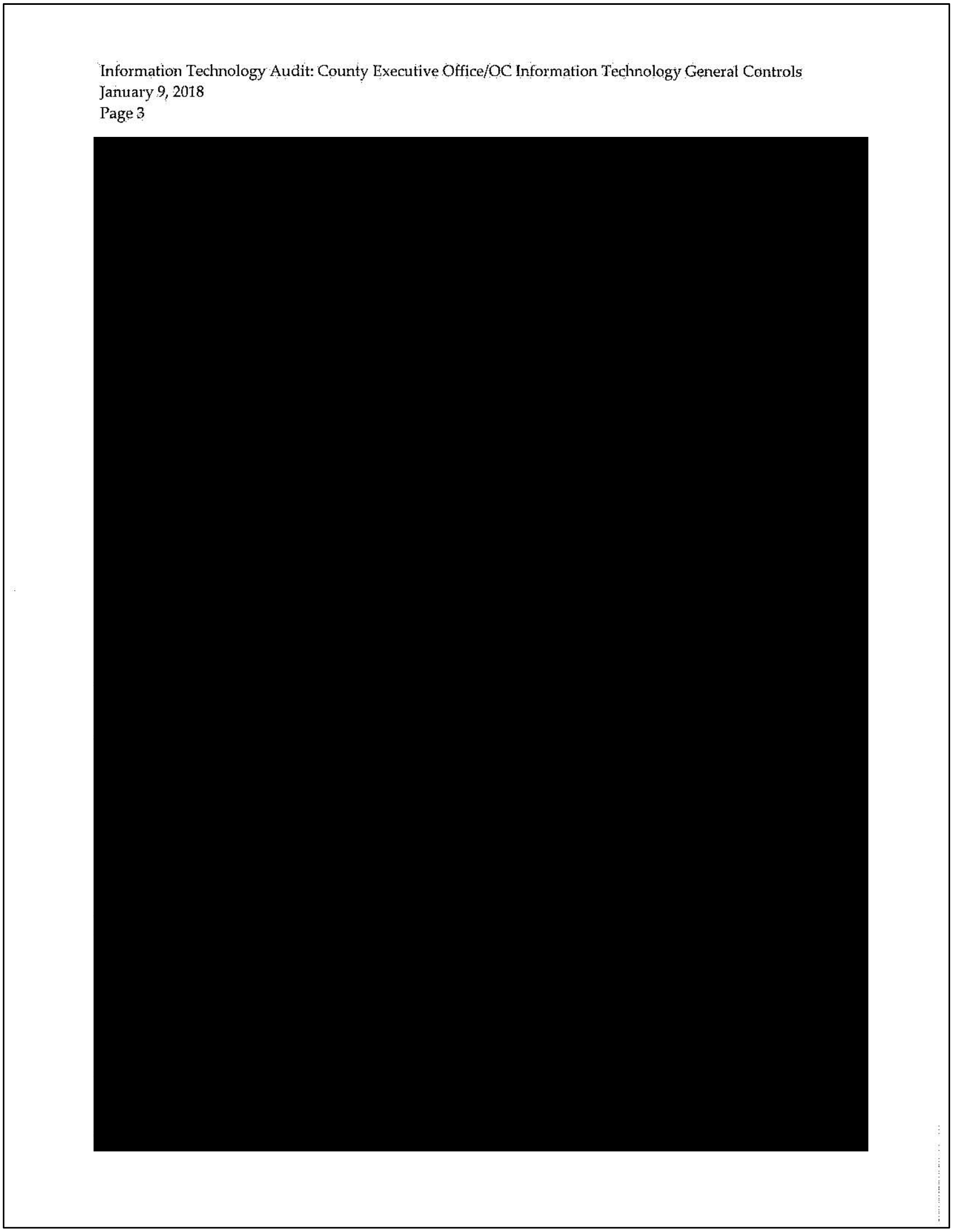
In conclusion, the audit identified 31 findings. OCIT has already addressed many of the findings and will be working to address any remaining action items and recommendations over the next 3 – 6 months. These findings will aid in continuing to provide quality IT services for the County. Taking into consideration the extensive size and scope of the services OCIT provides, the number and type of audit findings are well within acceptable norms for an IT organization of this type.

Attached are OCIT's responses to the report.

Should you have questions or concerns with regards to cyber security audits and assessment services, do not hesitate to contact me, Joel Golub, Chief Information Officer, at (714) 834-6827.

cc: Jacob Margolis, Chief Information Security Officer
KC Roestenberg, Assistant CIO
Bob Berg, Director of Infrastructure and Communication Services
Jayesh Patel, Director of Applications Development & Support
Clyde Gamboa, Director of Technology

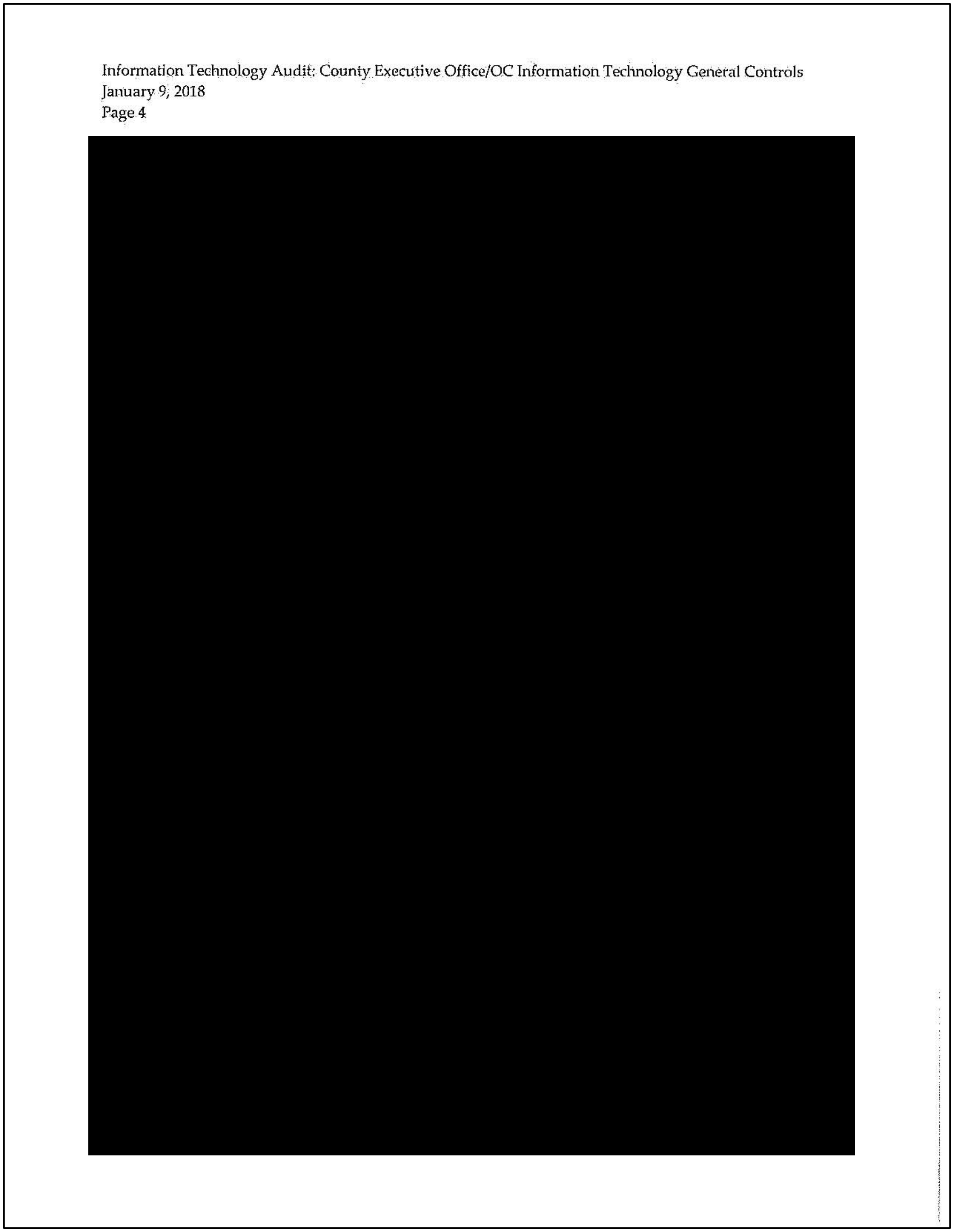
ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



Information Technology Audit: County Executive Office/OC Information Technology General Controls
January 9, 2018
Page 3

[redacted]

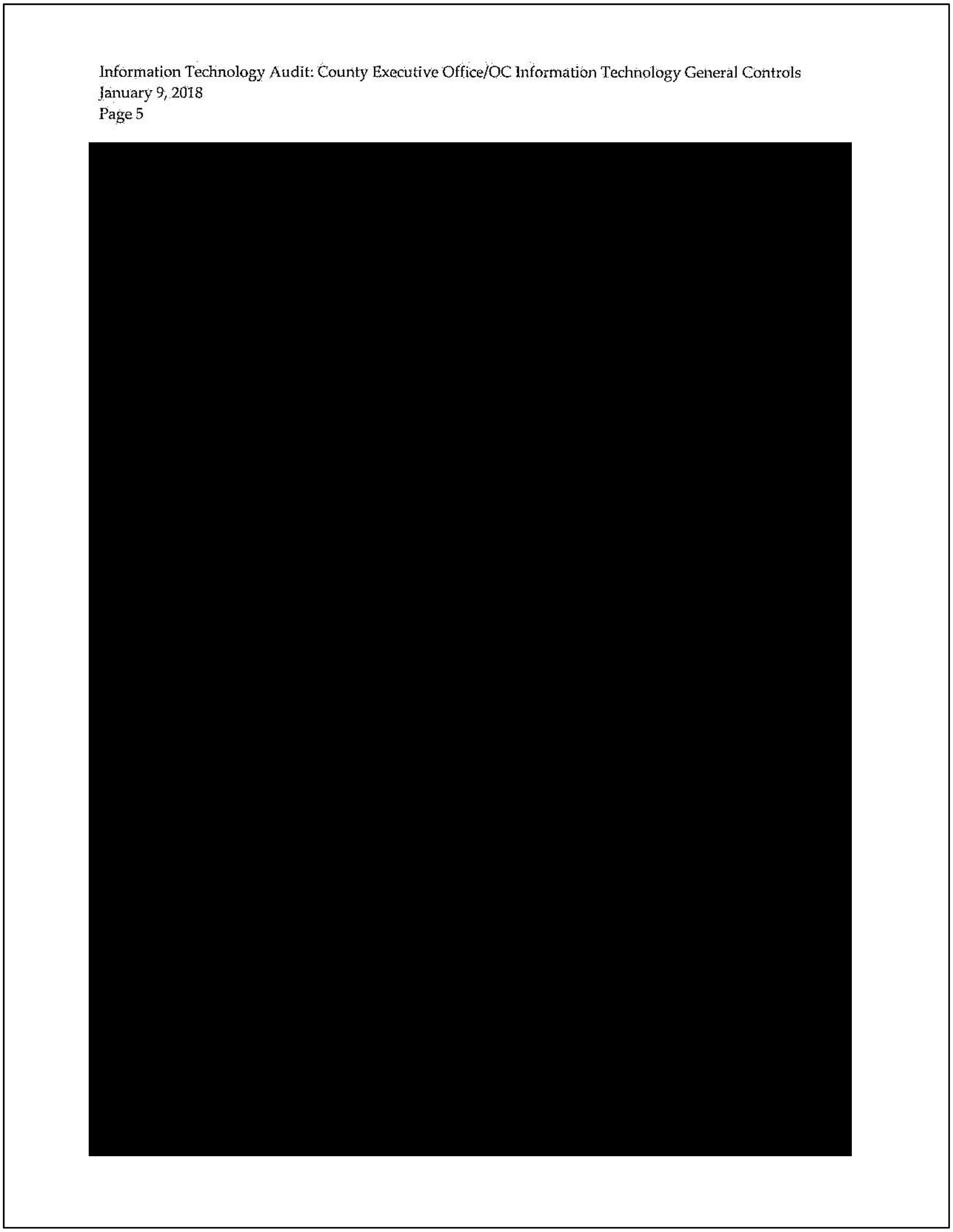
ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



Information Technology Audit: County Executive Office/OC Information Technology General Controls
January 9, 2018
Page 4

[redacted]

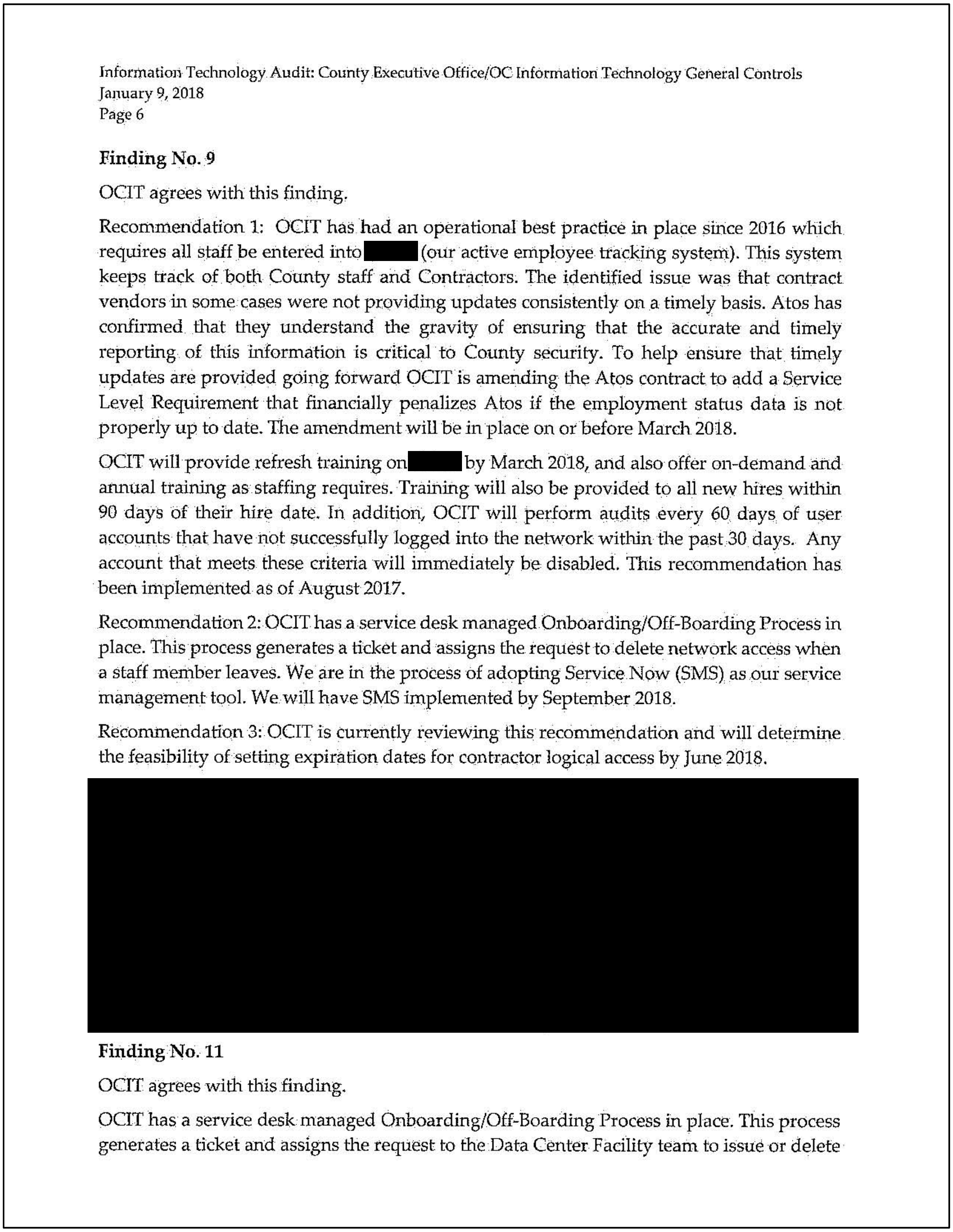
ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



Information Technology Audit: County Executive Office/OC Information Technology General Controls
January 9, 2018
Page 5

[redacted]

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



Information Technology Audit: County Executive Office/OC Information Technology General Controls
January 9, 2018
Page 6

Finding No. 9

OCIT agrees with this finding.

Recommendation 1: OCIT has had an operational best practice in place since 2016 which requires all staff be entered into [redacted] (our active employee tracking system). This system keeps track of both County staff and Contractors. The identified issue was that contract vendors in some cases were not providing updates consistently on a timely basis. Atos has confirmed that they understand the gravity of ensuring that the accurate and timely reporting of this information is critical to County security. To help ensure that timely updates are provided going forward OCIT is amending the Atos contract to add a Service Level Requirement that financially penalizes Atos if the employment status data is not properly up to date. The amendment will be in place on or before March 2018.

OCIT will provide refresh training on [redacted] by March 2018, and also offer on-demand and annual training as staffing requires. Training will also be provided to all new hires within 90 days of their hire date. In addition, OCIT will perform audits every 60 days of user accounts that have not successfully logged into the network within the past 30 days. Any account that meets these criteria will immediately be disabled. This recommendation has been implemented as of August 2017.

Recommendation 2: OCIT has a service desk managed Onboarding/Off-Boarding Process in place. This process generates a ticket and assigns the request to delete network access when a staff member leaves. We are in the process of adopting Service Now (SMS) as our service management tool. We will have SMS implemented by September 2018.

Recommendation 3: OCIT is currently reviewing this recommendation and will determine the feasibility of setting expiration dates for contractor logical access by June 2018.

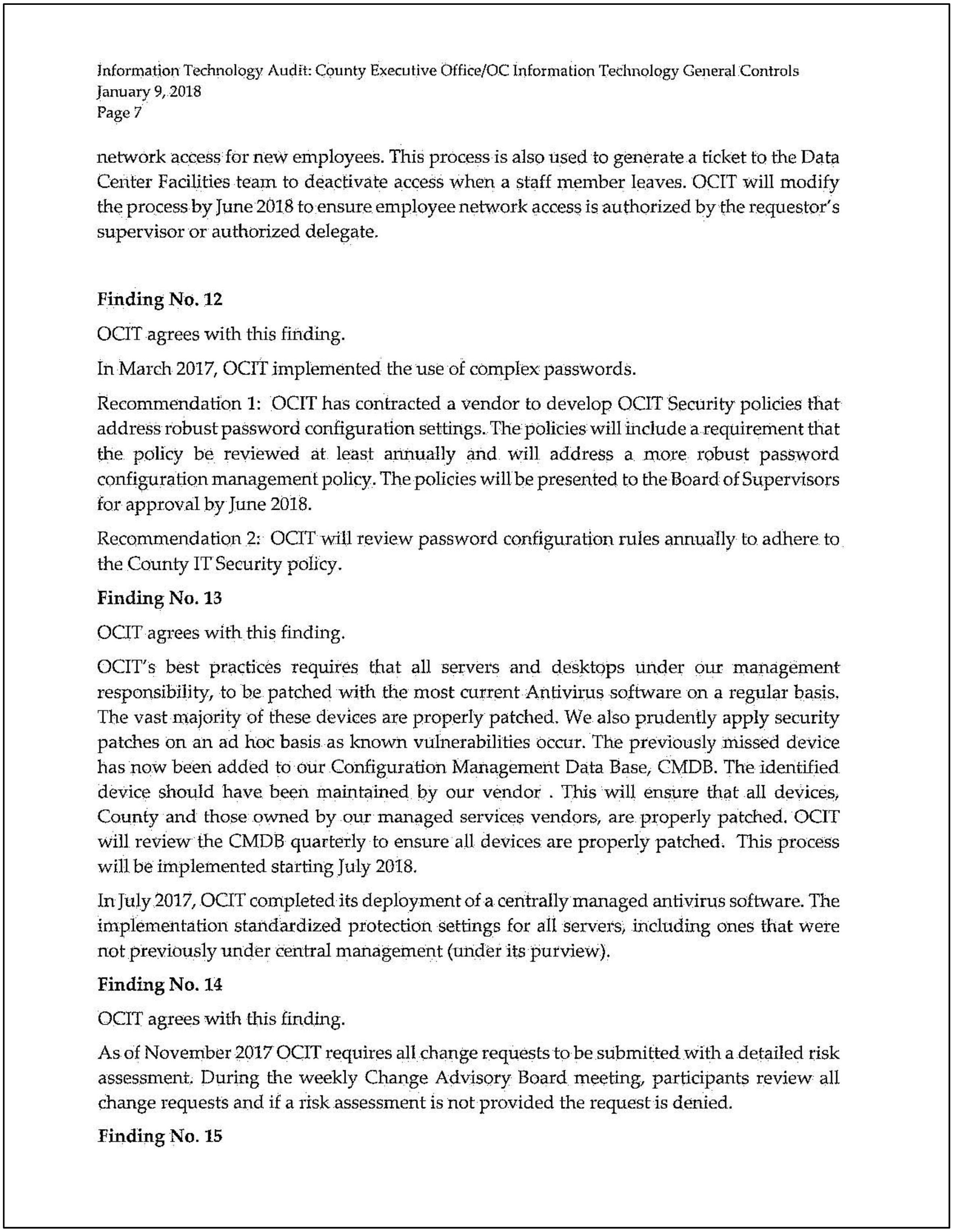
[redacted]

Finding No. 11

OCIT agrees with this finding.

OCIT has a service desk managed Onboarding/Off-Boarding Process in place. This process generates a ticket and assigns the request to the Data Center Facility team to issue or delete

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



network access for new employees. This process is also used to generate a ticket to the Data Center Facilities team to deactivate access when a staff member leaves. OCIT will modify the process by June 2018 to ensure employee network access is authorized by the requestor's supervisor or authorized delegate.

Finding No. 12

OCIT agrees with this finding.

In March 2017, OCIT implemented the use of complex passwords.

Recommendation 1: OCIT has contracted a vendor to develop OCIT Security policies that address robust password configuration settings. The policies will include a requirement that the policy be reviewed at least annually and will address a more robust password configuration management policy. The policies will be presented to the Board of Supervisors for approval by June 2018.

Recommendation 2: OCIT will review password configuration rules annually to adhere to the County IT Security policy.

Finding No. 13

OCIT agrees with this finding.

OCIT's best practices requires that all servers and desktops under our management responsibility, to be patched with the most current Antivirus software on a regular basis. The vast majority of these devices are properly patched. We also prudently apply security patches on an ad hoc basis as known vulnerabilities occur. The previously missed device has now been added to our Configuration Management Data Base, CMDB. The identified device should have been maintained by our vendor . This will ensure that all devices, County and those owned by our managed services vendors, are properly patched. OCIT will review the CMDB quarterly to ensure all devices are properly patched. This process will be implemented starting July 2018.

In July 2017, OCIT completed its deployment of a centrally managed antivirus software. The implementation standardized protection settings for all servers, including ones that were not previously under central management (under its purview).

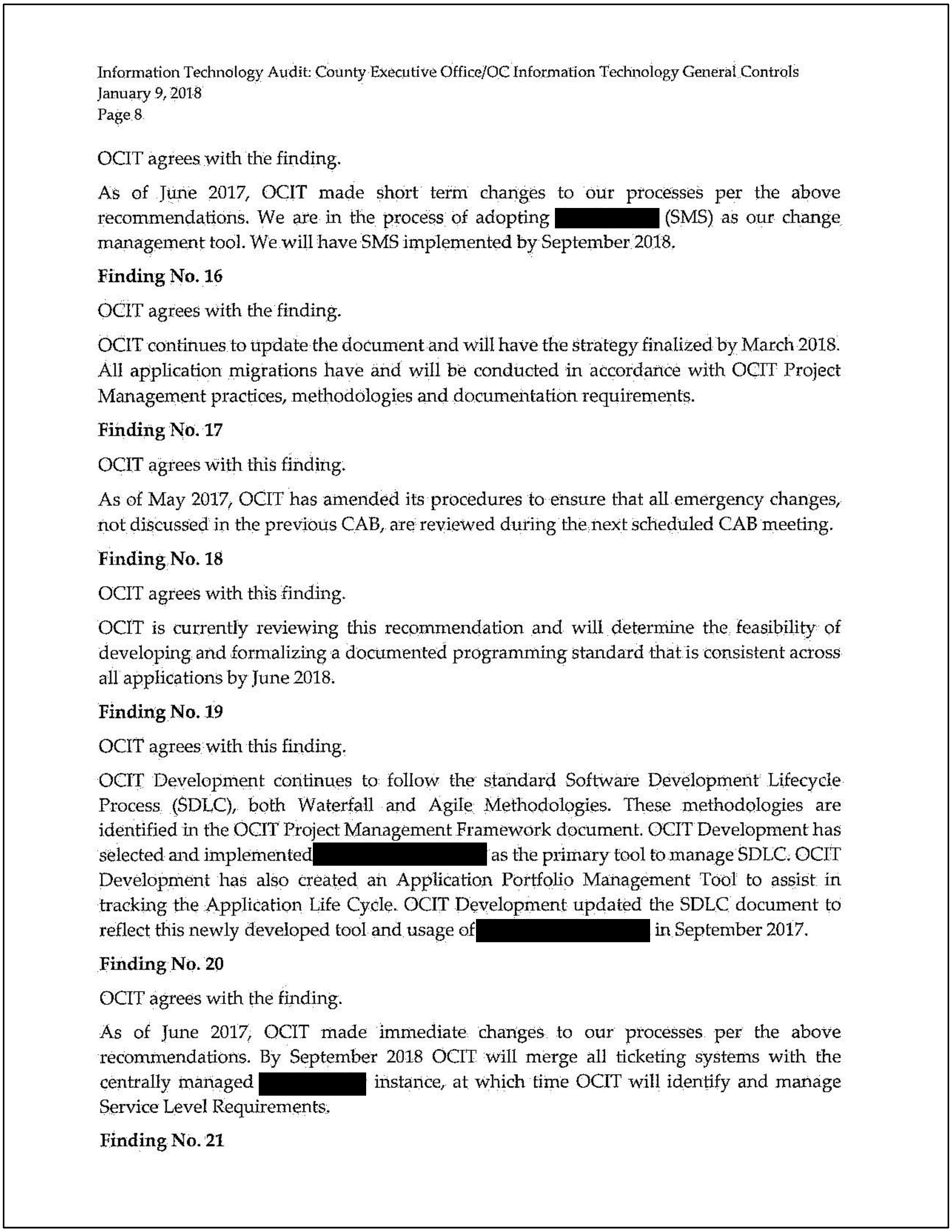
Finding No. 14

OCIT agrees with this finding.

As of November 2017 OCIT requires all change requests to be submitted with a detailed risk assessment. During the weekly Change Advisory Board meeting, participants review all change requests and if a risk assessment is not provided the request is denied.

Finding No. 15

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



Information Technology Audit: County Executive Office/OC Information Technology General Controls
January 9, 2018
Page 8

OCIT agrees with the finding.

As of June 2017, OCIT made short term changes to our processes per the above recommendations. We are in the process of adopting [redacted] (SMS) as our change management tool. We will have SMS implemented by September 2018.

Finding No. 16

OCIT agrees with the finding.

OCIT continues to update the document and will have the strategy finalized by March 2018. All application migrations have and will be conducted in accordance with OCIT Project Management practices, methodologies and documentation requirements.

Finding No. 17

OCIT agrees with this finding.

As of May 2017, OCIT has amended its procedures to ensure that all emergency changes, not discussed in the previous CAB, are reviewed during the next scheduled CAB meeting.

Finding No. 18

OCIT agrees with this finding.

OCIT is currently reviewing this recommendation and will determine the feasibility of developing and formalizing a documented programming standard that is consistent across all applications by June 2018.

Finding No. 19

OCIT agrees with this finding.

OCIT Development continues to follow the standard Software Development Lifecycle Process (SDLC), both Waterfall and Agile Methodologies. These methodologies are identified in the OCIT Project Management Framework document. OCIT Development has selected and implemented [redacted] as the primary tool to manage SDLC. OCIT Development has also created an Application Portfolio Management Tool to assist in tracking the Application Life Cycle. OCIT Development updated the SDLC document to reflect this newly developed tool and usage of [redacted] in September 2017.

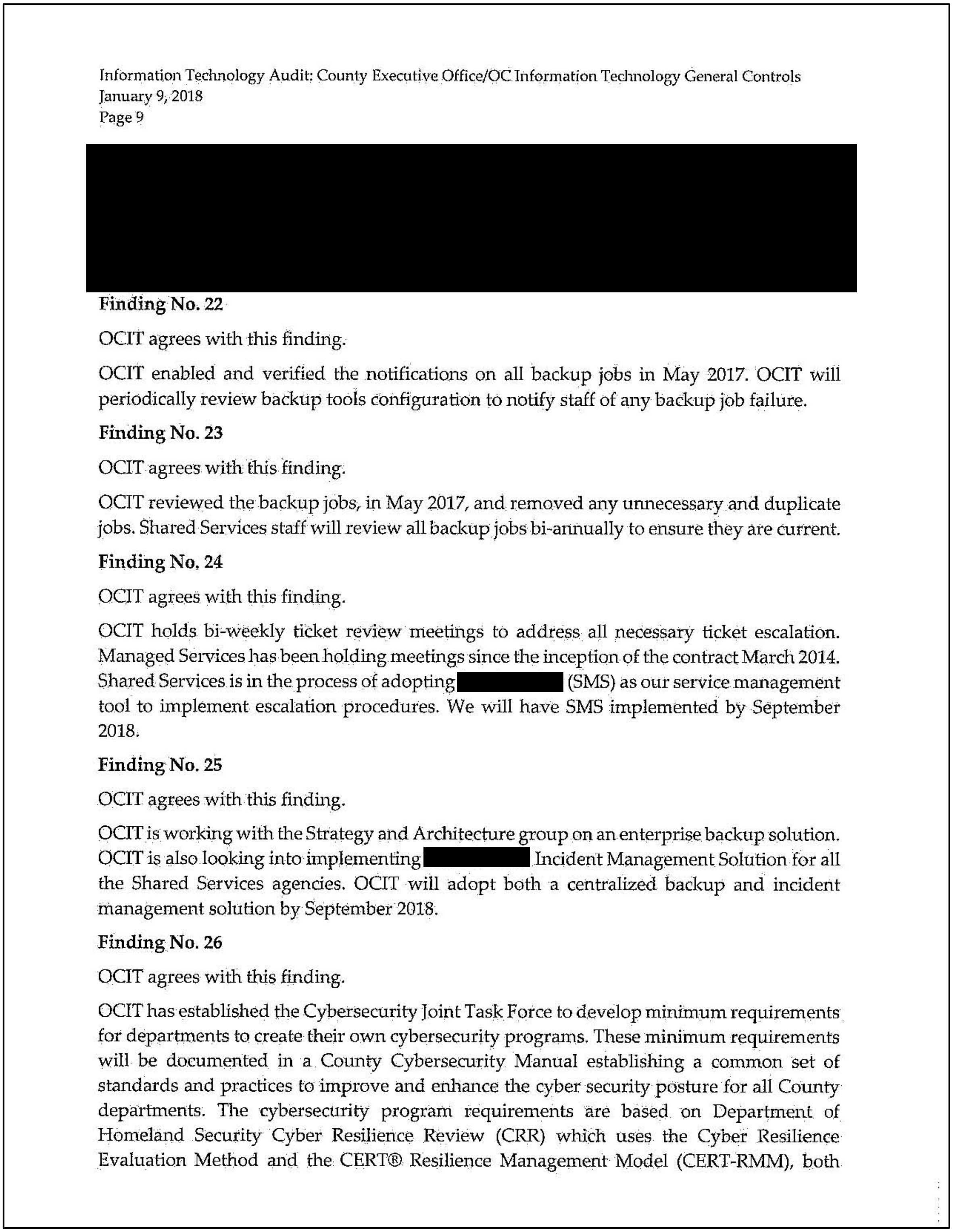
Finding No. 20

OCIT agrees with the finding.

As of June 2017, OCIT made immediate changes to our processes per the above recommendations. By September 2018 OCIT will merge all ticketing systems with the centrally managed [redacted] instance, at which time OCIT will identify and manage Service Level Requirements.

Finding No. 21

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



[redacted]

Finding No. 22

OCIT agrees with this finding.

OCIT enabled and verified the notifications on all backup jobs in May 2017. OCIT will periodically review backup tools configuration to notify staff of any backup job failure.

Finding No. 23

OCIT agrees with this finding.

OCIT reviewed the backup jobs, in May 2017, and removed any unnecessary and duplicate jobs. Shared Services staff will review all backup jobs bi-annually to ensure they are current.

Finding No. 24

OCIT agrees with this finding.

OCIT holds bi-weekly ticket review meetings to address all necessary ticket escalation. Managed Services has been holding meetings since the inception of the contract March 2014. Shared Services is in the process of adopting [redacted] (SMS) as our service management tool to implement escalation procedures. We will have SMS implemented by September 2018.

Finding No. 25

OCIT agrees with this finding.

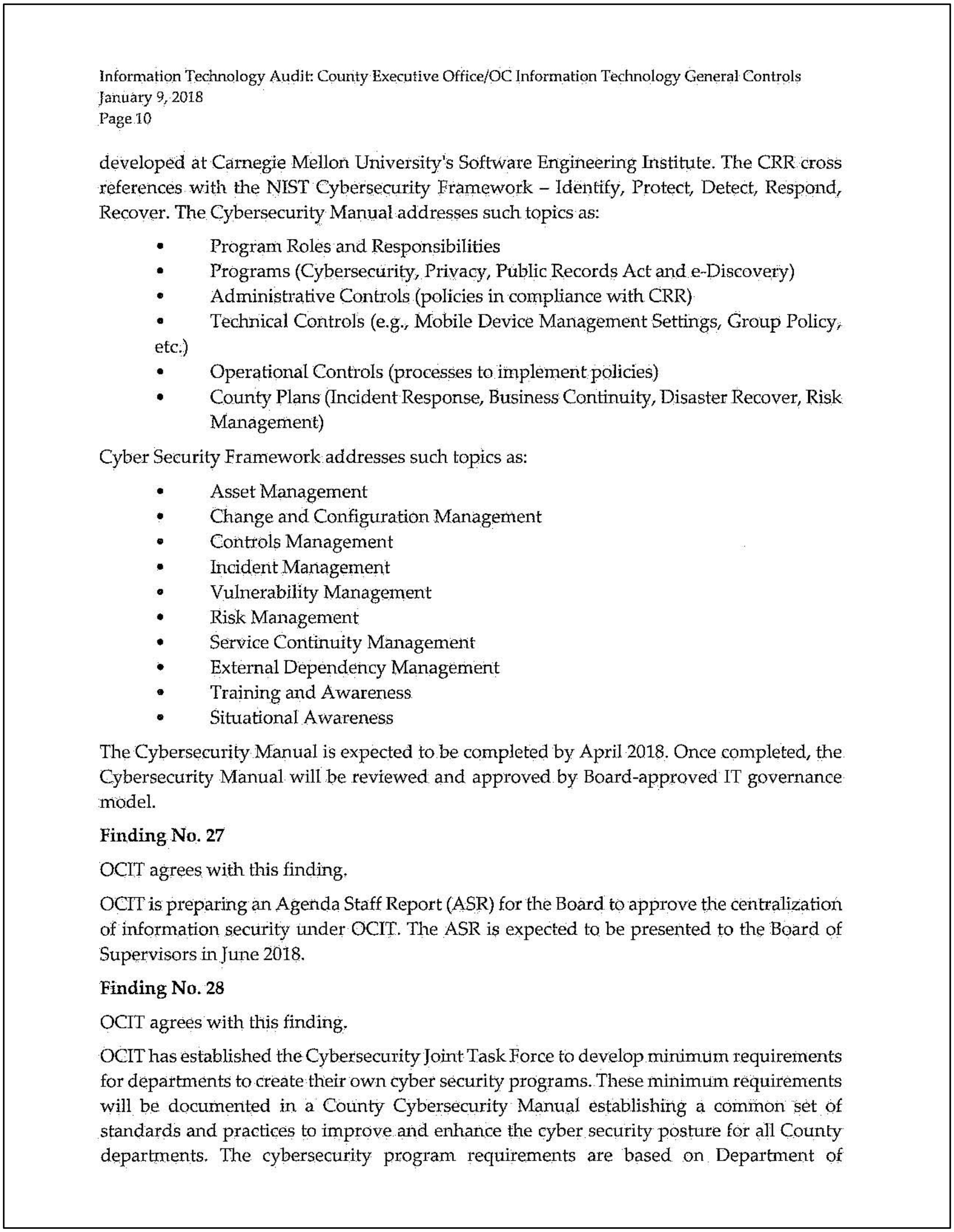
OCIT is working with the Strategy and Architecture group on an enterprise backup solution. OCIT is also looking into implementing [redacted] Incident Management Solution for all the Shared Services agencies. OCIT will adopt both a centralized backup and incident management solution by September 2018.

Finding No. 26

OCIT agrees with this finding.

OCIT has established the Cybersecurity Joint Task Force to develop minimum requirements for departments to create their own cybersecurity programs. These minimum requirements will be documented in a County Cybersecurity Manual establishing a common set of standards and practices to improve and enhance the cyber security posture for all County departments. The cybersecurity program requirements are based on Department of Homeland Security Cyber Resilience Review (CRR) which uses the Cyber Resilience Evaluation Method and the CERT® Resilience Management Model (CERT-RMM), both

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



developed at Carnegie Mellon University's Software Engineering Institute. The CRR cross references with the NIST Cybersecurity Framework – Identify, Protect, Detect, Respond, Recover. The Cybersecurity Manual addresses such topics 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, etc.)
- Operational Controls (processes to implement policies)
- County Plans (Incident Response, Business Continuity, Disaster Recover, Risk Management)

Cyber Security Framework addresses such topics as:

- Asset Management
- Change and Configuration Management
- Controls Management
- Incident Management
- Vulnerability Management
- Risk Management
- Service Continuity Management
- External Dependency Management
- Training and Awareness
- Situational Awareness

The Cybersecurity Manual is expected to be completed by April 2018. Once completed, the Cybersecurity Manual will be reviewed and approved by Board-approved IT governance model.

Finding No. 27

OCIT agrees with this finding.

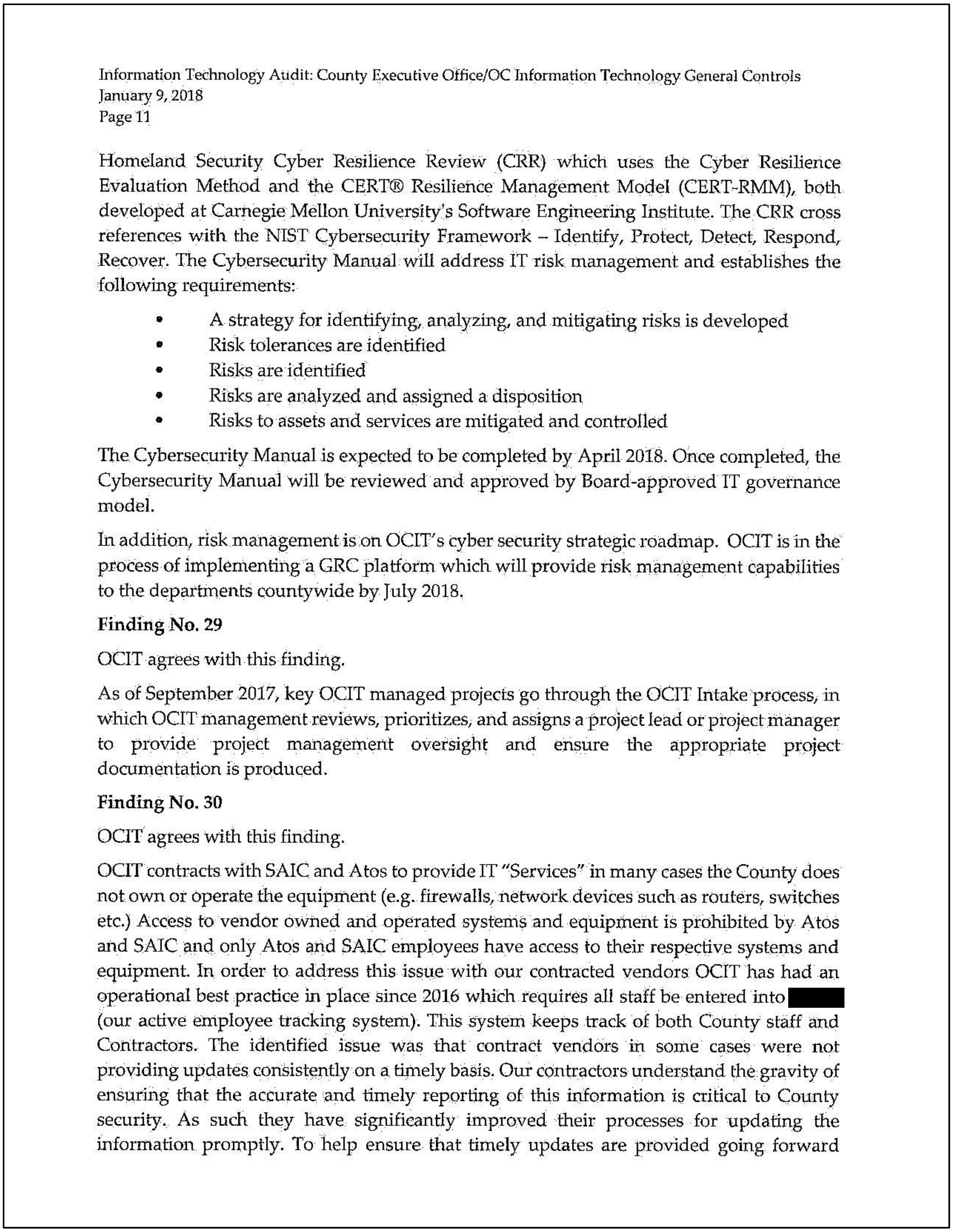
OCIT is preparing an Agenda Staff Report (ASR) for the Board to approve the centralization of information security under OCIT. The ASR is expected to be presented to the Board of Supervisors in June 2018.

Finding No. 28

OCIT agrees with this finding.

OCIT has established the Cybersecurity Joint Task Force to develop minimum requirements for departments to create their own cyber security programs. These minimum requirements will be documented in a County Cybersecurity Manual establishing a common set of standards and practices to improve and enhance the cyber security posture for all County departments. The cybersecurity program requirements are based on Department of

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



Homeland Security Cyber Resilience Review (CRR) which uses the Cyber Resilience Evaluation Method and the CERT® Resilience Management Model (CERT-RMM), both developed at Carnegie Mellon University's Software Engineering Institute. The CRR cross references with the NIST Cybersecurity Framework – Identify, Protect, Detect, Respond, Recover. The Cybersecurity Manual will address IT risk management and establishes the following requirements:

- A strategy for identifying, analyzing, and mitigating risks is developed
- Risk tolerances are identified
- Risks are identified
- Risks are analyzed and assigned a disposition
- Risks to assets and services are mitigated and controlled

The Cybersecurity Manual is expected to be completed by April 2018. Once completed, the Cybersecurity Manual will be reviewed and approved by Board-approved IT governance model.

In addition, risk management is on OCIT's cyber security strategic roadmap. OCIT is in the process of implementing a GRC platform which will provide risk management capabilities to the departments countywide by July 2018.

Finding No. 29

OCIT agrees with this finding.

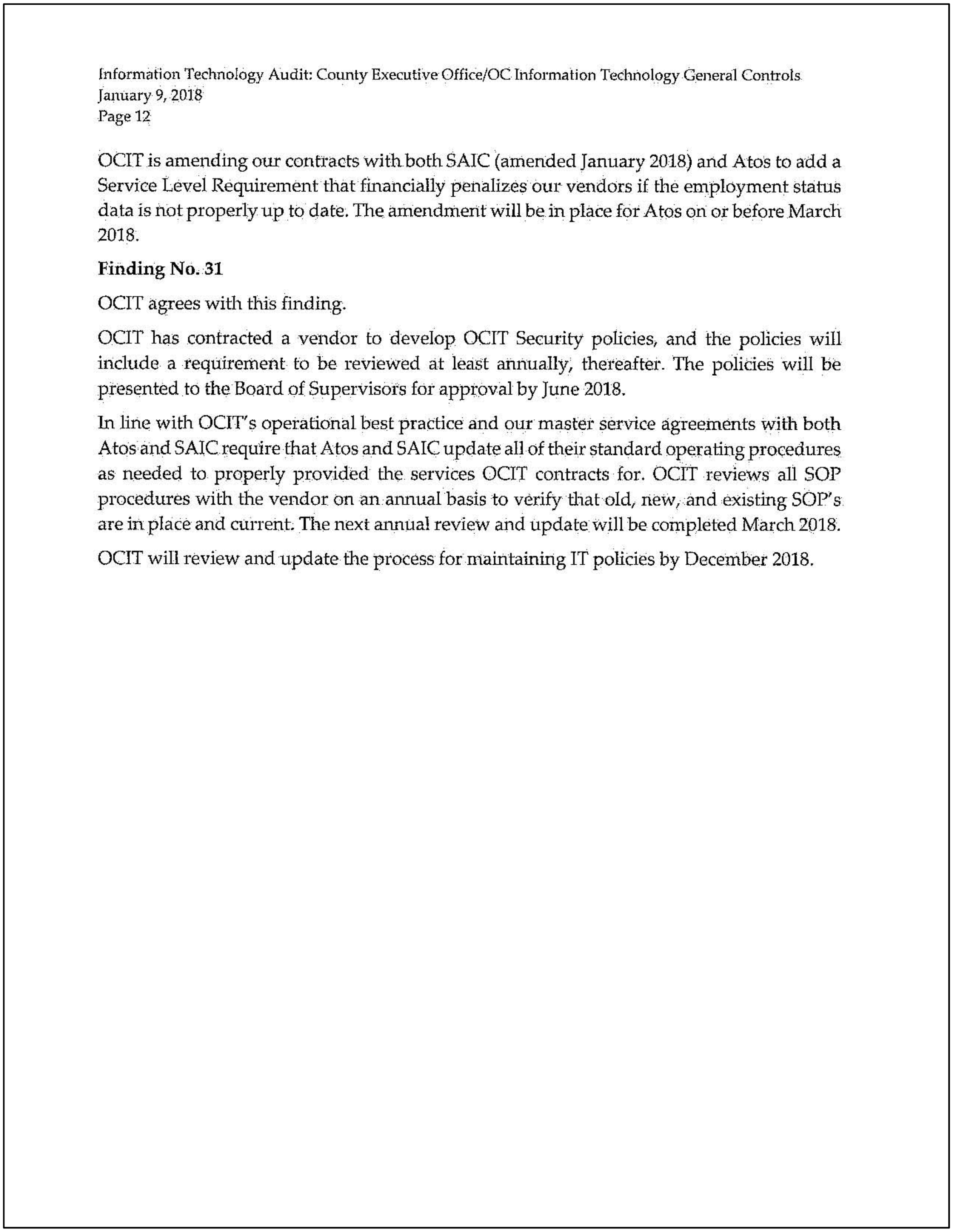
As of September 2017, key OCIT managed projects go through the OCIT Intake process, in which OCIT management reviews, prioritizes, and assigns a project lead or project manager to provide project management oversight and ensure the appropriate project documentation is produced.

Finding No. 30

OCIT agrees with this finding.

OCIT contracts with SAIC and Atos to provide IT "Services" in many cases the County does not own or operate the equipment (e.g. firewalls, network devices such as routers, switches etc.) Access to vendor owned and operated systems and equipment is prohibited by Atos and SAIC and only Atos and SAIC employees have access to their respective systems and equipment. In order to address this issue with our contracted vendors OCIT has had an operational best practice in place since 2016 which requires all staff be entered into [redacted] (our active employee tracking system). This system keeps track of both County staff and Contractors. The identified issue was that contract vendors in some cases were not providing updates consistently on a timely basis. Our contractors understand the gravity of ensuring that the accurate and timely reporting of this information is critical to County security. As such they have significantly improved their processes for updating the information promptly. To help ensure that timely updates are provided going forward

ATTACHMENT B: County Executive Office/OC Information Technology Management Responses (cont.)



Information Technology Audit: County Executive Office/OC Information Technology General Controls
January 9, 2018
Page 12

OCIT is amending our contracts with both SAIC (amended January 2018) and Atos to add a Service Level Requirement that financially penalizes our vendors if the employment status data is not properly up to date. The amendment will be in place for Atos on or before March 2018.

Finding No. 31

OCIT agrees with this finding.

OCIT has contracted a vendor to develop OCIT Security policies, and the policies will include a requirement to be reviewed at least annually, thereafter. The policies will be presented to the Board of Supervisors for approval by June 2018.

In line with OCIT's operational best practice and our master service agreements with both Atos and SAIC require that Atos and SAIC update all of their standard operating procedures as needed to properly provided the services OCIT contracts for. OCIT reviews all SOP procedures with the vendor on an annual basis to verify that old, new, and existing SOP's are in place and current. The next annual review and update will be completed March 2018.

OCIT will review and update the process for maintaining IT policies by December 2018.