LOS ANGELES COUNTY
AUDITOR-CONTROLLER

Arlene Barrera
ACTING AUDITOR-CONTROLLER

Peter Hughes
ASSISTANT AUDITOR-CONTROLLER

Mike Pirolo
ACTING DIVISION CHIEF

AUDIT DIVISION

July 10, 2019

Los Angeles County Library
INFORMATION TECHNOLOGY AND SECURITY REVIEW

Audit Team

Michelle Romero, CIA
Principal Accountant-Auditor

Jayson Chan
Senior Accountant-Auditor

NUMBER OF RECOMMENDATIONS

PRIORITY 1
1
CORRECTIVE ACTION REQUIRED WITHIN 90 DAYS

PRIORITY 2
7
CORRECTIVE ACTION REQUIRED WITHIN 120 DAYS

PRIORITY 3
2
CORRECTIVE ACTION REQUIRED WITHIN 180 DAYS

REPORT #K19BC

LOS ANGELES COUNTY
AUDITOR-CONTROLLER

Arlene Barrera
ACTING AUDITOR-CONTROLLER

Peter Hughes
ASSISTANT AUDITOR-CONTROLLER

Mike Pirolo
ACTING DIVISION CHIEF

AUDIT DIVISION

July 10, 2019

FACT SHEET

Los Angeles County Library

INFORMATION TECHNOLOGY AND SECURITY REVIEW

With the support and active participation of Los Angeles County Library (Library or Department) management and staff, we evaluated the design of Library's Information Technology (IT) and security procedures and controls to determine whether they provide reasonable assurance to management that devices have the proper security software protection, confidentiality and integrity of systems and data is maintained, and that employees are trained on IT security in accordance with the Board of Supervisors' IT and Security Policies, IT standards, and County Fiscal Manual requirements.

Key Outcomes

We noted various opportunities to improve and strengthen Library's information security processes, controls, and control monitoring, which management has agreed to strengthen. We will assess and report on management's corrective actions in our planned future follow-up review. Examples of corrective actions include:

- Library will implement processes to ensure all IT devices are encrypted and have current antivirus software protection.
- Library will implement processes to ensure encryption keys used to unencrypt IT devices are restricted to authorized users with a business need and stored in a secure manner.
- Library will implement ongoing self-monitoring processes to ensure controls are in place and working as intended, document the monitoring activity, elevate material exceptions to management, and ensure corrective actions are implemented as appropriate.

Impact

These enhancements will provide greater assurance of compliance with County IT rules; reduce the likelihood of unauthorized and/or incompatible software updates and lessen the potential for the exposure of confidential and/or sensitive County data.

FAST FACTS

Library has 87 community libraries serving 3.4 million residents in over 3,000 square miles.

Library reported over 1,300 employees, approximately 8,600 IT devices, and two critical IT systems, including the Integrated Library System, which is used for Library operations (e.g., fines/fees accounting).

NUMBER OF RECOMMENDATIONS

PRIORITY 1
1
CORRECTIVE ACTION REQUIRED WITHIN 90 DAYS

PRIORITY 2
7
CORRECTIVE ACTION REQUIRED WITHIN 120 DAYS

PRIORITY 3
2
CORRECTIVE ACTION REQUIRED WITHIN 180 DAYS

ACIS
Audit
Contract Monitoring
Investigation
Services

This report is also available online at auditor.lacounty.gov
Report Waste, Fraud, and Abuse: fraud.lacounty.gov

For questions regarding the contents of this report, please contact Mike Pirolo, Acting Audit Division Chief, at mpirolo@auditor.lacounty.gov or (213) 253-0100.

REPORT #K19BC

COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

ARLENE BARRERA
ACTING AUDITOR-CONTROLLER

July 10, 2019

TO: Supervisor Janice Hahn, Chair
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Kathryn Barger

FROM: Arlene Barrera
Acting Auditor-Controller

SUBJECT: **LOS ANGELES COUNTY LIBRARY – INFORMATION TECHNOLOGY AND SECURITY REVIEW**

The Auditor-Controller's Audit Division has completed a review of the Los Angeles County Library's (Library or Department) information technology and security operations. The complete audit report is attached.

If you have any questions please call me, or your staff may contact Mike Pirolo at (213) 253-0100.

AB:PH:MP

Attachments (Report #K19BC)

c: Sachi A. Hamai, Chief Executive Officer
Skye Patrick, County Librarian
William S. Kehoe, Chief Information Officer, Chief Executive Office
Ralph Johnson, Chief Information Security Officer, Chief Executive Office
Audit Committee
Countywide Communications

COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

ARLENE BARRERA
ACTING AUDITOR-CONTROLLER

ADDRESS ALL CORRESPONDENCE TO:
AUDIT DIVISION
350 S. FIGUEROA ST., 8th FLOOR
LOS ANGELES, CA 90071-1304

July 10, 2019

TO: Skye Patrick, County Librarian
Los Angeles County Library

FROM: Dr. Peter Hughes
Assistant Auditor-Controller

Mike Pirolo, Acting Chief
Audit Division

SUBJECT: **LOS ANGELES COUNTY LIBRARY – INFORMATION TECHNOLOGY AND SECURITY REVIEW**

We have completed a review of the Los Angeles County Library's (Library or Department) information technology and security operations. For details of our review, please see Attachment I, Table of Findings and Recommendations for Corrective Action and Attachment II, Background and Audit Scope.

Review of Report

We discussed our report with Library management. The Department's response (Attachment III) indicates general agreement with our findings and recommendations.

We thank Library management and staff for their cooperation and assistance during our review. If you have any questions, please call Mike Pirolo at (213) 253-0100.

PH:MP:mr

Attachments

c: Arlene Barrera, Acting Auditor-Controller

LOS ANGELES COUNTY LIBRARY – INFORMATION TECHNOLOGY AND SECURITY REVIEW

TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION

	ISSUE[1]	RISK	RECOMMENDATION	P[2]	SUMMARY OF RESPONSE
1	**Encryption and Antivirus Software Protection:** The Los Angeles County Library (Library or Department) needs to enhance their encryption and antivirus software processes and controls to ensure all information technology (IT) devices are encrypted and have antivirus software installed, as required by the Board of Supervisors' (Board) IT and Security Policy 6.102. Library indicated staff install encryption and antivirus software on all IT devices prior to deployment. However, there is no control to confirm the antivirus and encryption software was installed and is working properly on each device. Library also needs to periodically review and ensure all IT devices remain encrypted and have current antivirus software protection.	• Increased risk for unprotected IT devices and the potential exposure of County data.	**Library management enhance their encryption and antivirus software protection processes and controls to ensure all IT devices are encrypted and have current antivirus software.**	1	**Agree** Target Implementation Date: August 30, 2019 Library's response indicates they will enhance their encryption and antivirus software protection processes and controls to ensure all IT devices are encrypted and have current antivirus software by implementing new protection software, documenting the installations, and conducting periodic reviews of the software status.
2	**Encryption Keys:** Library needs to establish processes to ensure encryption keys are restricted to users with a business need and stored in a secure manner, as required by the Countywide Baseline Encryption Standard for Computing Devices. Encryption keys are used to unencrypt IT devices and should be restricted to authorized users with a business need. We noted Library stores encryption keys in an unencrypted format in a network folder that is shared with all IT staff. This allows any IT staff, including staff that do not have a business need for encryption keys, to view and copy the keys to their device.	• Increased risk for unauthorized access to encryption keys and for the potential exposure of County data.	**Library management establish processes to ensure encryption keys are restricted to users with a business need and stored in a secure manner.**	2	**Agree** Target Implementation Date: October 15, 2019 Library's response indicates they will establish processes to ensure encryption keys are restricted to system and network administrators and stored in a secure server.

[1] For background information about the processes reviewed, please refer to the Process Overview section in Attachment II.

[2] **Priority Ranking:** Recommendations are ranked from Priority 1 to Priority 3 based on the potential seriousness and likelihood of negative impact on departmental operations if corrective action is not taken. See Attachment IV for definitions of priority rankings.

TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION					
	ISSUE[1]	RISK	RECOMMENDATION	P[2]	SUMMARY OF RESPONSE
3	**Password Controls:** Library needs to evaluate implementing password controls for their network and the Integrated Library System (ILS), as required by County Fiscal Manual (CFM) Section 8.7.4.3. The ILS is used to support Library operations, including the circulation and acquisition of library materials, library catalog, fines/fees accounting, customer account management, and access to online reference databases. Specifically, during our interviews and walkthroughs, we noted password complexity requirements (i.e., minimum length and a combination of numeric, upper, and lower-case characters) are not in place, logon identifications (ID) are not suspended after any number of invalid logon attempts, and users are never required to change their passwords. In addition, we observed users sharing passwords.	• Increased risk for unauthorized access to IT resources and inappropriate network and ILS activity.	**Library management evaluate implementing password controls for their network and ILS.**	2	**Agree** Target Implementation Date: September 15, 2019 Library's response indicates they will implement password controls for their network and ILS that enforces password complexity requirements, suspends user accounts after three failed logon attempts, changes passwords every 90 days, and prohibits password sharing.
4	**User Access IDs:** Library does not always require unique user logon IDs to access their network, as required by CFM 8.7.4.3. While unique ID's are generally required to access the network, during our interviews and walkthroughs, we observed individuals sharing generic logon IDs for privileged network access (i.e., administrative rights). Logon IDs should be unique to each user to establish accountability and provide an audit trail of user activity.	• Increased risk for unauthorized access to IT resources and lack of an audit trail to establish accountability over user activity.	**Library management require unique user logon IDs to access their network.**	2	**Agree** Target Implementation Date: August 15, 2019 Library's response indicates they will ensure network logon IDs are unique to each user.

[1] For background information about the processes reviewed, please refer to the Process Overview section in Attachment II.

[2] **Priority Ranking:** Recommendations are ranked from Priority 1 to Priority 3 based on the potential seriousness and likelihood of negative impact on departmental operations if corrective action is not taken. See Attachment IV for definitions of priority rankings.

TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION					
	ISSUE[1]	RISK	RECOMMENDATION	P[2]	SUMMARY OF RESPONSE
5	**User Access Reviews:** Library needs to establish a process to review network and ILS user access rights quarterly to ensure accounts are authorized and access capabilities remain consistent with users' job duties, as required by CFM Section 8.7.4.2. This should include a review of users with the ability to access sensitive and confidential information, such as customer addresses and delinquent account information and privileged users with the ability to grant and remove network access.	• Increased risk for unauthorized access to the Department's network, which can lead to the exposure of confidential or sensitive County data.	**Library management establish a process to perform and document quarterly user access reviews.**	2	**Agree** Target Implementation Date: October 15, 2019 Library's response indicates they will establish a process to perform quarterly user access reviews of all users, including privileged users.
6	**IT Security Training:** Library needs to establish training processes and controls to train all employees annually on IT security and document their participation, as required by Board Policy 6.100. Library management indicated they periodically provide IT security tips and notifications to staff through e-mails, flyers, and pamphlets and have a process to train employees annually on IT security. However, they estimate only 50 percent of their staff have taken the annual training because of issues with their training system. Library management needs to train all employees annually on IT security and document their participation as required by Board Policies.	• Increased risk for security incidents, including data breaches and other issues. Insufficient training has been cited as a contributory factor in many recent significant public and private IT security incidents.	**Library management establish processes and controls to train all employees annually on IT security and document their participation.**	2	**Agree** Reported Implementation Date: April 11, 2019 Library's response indicates they implemented the new County IT security training software and will ensure all staff complete the training annually by reviewing status reports. **Auditor-Controller Response:** We will review Library's assertion that the recommendation is implemented during our follow-up review.

[1] For background information about the processes reviewed, please refer to the Process Overview section in Attachment II.

[2] **Priority Ranking:** Recommendations are ranked from Priority 1 to Priority 3 based on the potential seriousness and likelihood of negative impact on departmental operations if corrective action is not taken. See Attachment IV for definitions of priority rankings.

TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION					
	ISSUE[1]	RISK	RECOMMENDATION	P[2]	SUMMARY OF RESPONSE
7	**Physical Security Access:** Library needs to establish a process to periodically review that access to restricted IT areas is appropriate, as required by Board Policy 6.100. We noted access to libraries and warehouses, which store/maintain IT equipment, is restricted with keys and key cards. However, Library management indicated they do not periodically review users' access to determine if it is still appropriate/authorized.	• Increased risk for IT resources being tampered with, damaged, stolen, or accessed by unauthorized personnel and for unauthorized access to restricted IT areas to go undetected.	**Library management establish a process to periodically review that access to restricted IT areas is appropriate.**	2	**Agree** Reported Implementation Date: February 4, 2019 Library's response indicates they established a process to periodically review that access to restricted IT areas is appropriate. **Auditor-Controller Response:** We will review Library's assertion that the recommendation is implemented during our follow-up review.
8	**Annual Inventory Reconciliation:** Although the Department has a process to investigate discrepancies between the master IT equipment listing and the annual physical inventory counts, the reconciliation needs to be completed timely. During our interviews and walkthroughs, we noted Library conducted a physical count of their IT equipment in October 2017. However, as of August 2018, they had not completed their reconciliation of the physical counts to their master IT equipment list. The incomplete reconciliation may result in missing, lost, and/or stolen IT equipment that would not be identified, investigated, or reported to the appropriate parties timely, as required by Board Policies 6.102 and 6.103.	• Increased risk that incidents will not be investigated timely. • Increased risk for the loss or theft to go undetected; and for potential exposure of County data. • Penalties/fines may be imposed for unreported security incidents.	**Library management develop processes to ensure the master IT equipment listing and the annual physical inventory counts are reconciled timely.**	2	**Agree** Reported Implementation Date: January 29, 2019 Library's response indicates they developed processes to ensure the master IT equipment listing and the annual physical inventory counts are reconciled timely. **Auditor-Controller Response:** We will review Library's assertion that the recommendation is implemented during our follow-up review.

[1] For background information about the processes reviewed, please refer to the Process Overview section in Attachment II.

[2] **Priority Ranking:** Recommendations are ranked from Priority 1 to Priority 3 based on the potential seriousness and likelihood of negative impact on departmental operations if corrective action is not taken. See Attachment IV for definitions of priority rankings.

TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION					
	ISSUE[1]	RISK	RECOMMENDATION	P[2]	SUMMARY OF RESPONSE
9	**Management Monitoring of Internal Controls:** For the following areas, Library management needs to develop ongoing self-monitoring processes to regularly monitor and document that processes and controls are working as intended, as required by Board Policy 6.100 and CFM 1.0.2: • Encryption and antivirus protection, including software installation and periodic IT device reviews. • Network/System user access reviews. • IT security training compliance. • Physical security access reviews. Effective self-monitoring processes could include tests or observations examining an adequate number of transactions on a regular basis (e.g., 5 – 10, weekly, quarterly, or semi-annually) to ensure adherence to policy, rules and/or generally accepted control principles, and documenting and retaining evidence of this review in such a manner that a third party can subsequently validate it. The monitoring process should also ensure material exceptions are elevated to management to ensure awareness of relative control risk on a timely basis and to ensure appropriate corrective actions are implemented.	• Prevents management from having reasonable assurance that important departmental and County IT and security objectives are being achieved. • Increased risk for not promptly identifying and correcting any process and control weaknesses or instances of non-compliance with County IT and security rules, such as employee improprieties, unprotected devices, and inappropriate and unauthorized access to restricted IT areas.	**Library management develop ongoing self-monitoring processes to ensure controls function as intended that include:** **a) Examination of process and control activities, such as a review of an adequate number of transactions on a regular basis to ensure adherence to County rules.** **b) Documenting the monitoring activity and retaining evidence so it can be subsequently validated.** **c) Elevating material exceptions to management on a timely basis to ensure awareness of relative control risk and to ensure appropriate corrective actions are implemented.**	3	**Agree** Target Implementation Date: November 15, 2019 Library's response indicates they will establish processes to conduct quarterly management self-monitoring over encryption and antivirus protection, network and system user access reviews, IT security training, and physical security access.

[1] For background information about the processes reviewed, please refer to the Process Overview section in Attachment II.

[2] **Priority Ranking:** Recommendations are ranked from Priority 1 to Priority 3 based on the potential seriousness and likelihood of negative impact on departmental operations if corrective action is not taken. See Attachment IV for definitions of priority rankings.

TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION					
	ISSUE[1]	RISK	RECOMMENDATION	P[2]	SUMMARY OF RESPONSE
10	**Updated Standards and Procedures**: Library maintains a collection of thorough and detailed IT policies and procedures. However, Library needs to update their existing standards and procedures, as required by CFM 8.3.0, to include the following processes noted in this report: • Physical security, including processes to review all employees with physical keys and keycards to restricted IT areas to ensure their access is authorized and appropriate. • Access controls, including a process to monitor access to critical applications. • Public access computers, including processes to manage and monitor access and inform users of the expectations and responsibilities. Standards and procedures should provide detailed guidance to staff and supervisors in the performance of their day-to-day duties and describe how processes are performed. They must also require staff and supervisors to maintain documentation of their processes and require an audit trail of key events where practical. For example, procedures for Library's physical security access review process would describe duties, such as how to generate reports of users with access to restricted IT areas, how often this should be completed, and the documentation to be maintained.	• Increased risk that staff will perform tasks, such as the physical security access review process incorrectly or inconsistently and increased effort required to train new staff to perform these processes. • Prevents management from effectively evaluating processing/control environments. • Increased risk for deviations from processes designed by management to accomplish departmental objectives and/or enable compliance with County IT policies/rules.	**Library management update their written standards and procedures to adequately guide supervisors and staff in the performance of their duties for critical IT and security processes mentioned.**	3	**Agree** Target Implementation Date: November 15, 2019 Library's response indicates they will establish and update written standards and procedures over physical security, access controls, and the public access network and users.

[1] For background information about the processes reviewed, please refer to the Process Overview section in Attachment II.

[2] **Priority Ranking:** Recommendations are ranked from Priority 1 to Priority 3 based on the potential seriousness and likelihood of negative impact on departmental operations if corrective action is not taken. See Attachment IV for definitions of priority rankings.

LOS ANGELES COUNTY LIBRARY
INFORMATION TECHNOLOGY AND SECURITY REVIEW
BACKGROUND AND AUDIT SCOPE

WHAT PROMPTED THE REVIEW

As required by the Board of Supervisors' (Board) Information Technology (IT) and Security Policy (Policy) 6.105, IT Audit and Risk Assessment, we are reviewing County departments' IT and security processes for compliance with Board Policies and IT related security standards.

SCOPE AND OBJECTIVES

We reviewed the Los Angeles County Library's (Library or Department) IT and security processes and controls to determine whether they provide reasonable assurance to management that devices have the proper security software protection, confidentiality and integrity of systems and data is maintained, IT equipment is accurately accounted for and secure, and employees are trained on IT security in accordance with Board Policies, IT standards, and County Fiscal Manual (CFM) requirements. Our review included interviewing Library management and staff and reviewing procedures and controls over management monitoring/oversight, encryption and antivirus protection, system access control and authentication, IT security training, physical access to IT resources, IT equipment security, security incident response and reporting, IT risk assessment, and equipment disposition.

STANDARDS

We conducted our review in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

PROCESS OVERVIEW

The County's IT and security program is supported by Board Policies, IT standards, and the CFM and is designed to help protect County IT assets and ensure the confidentiality and integrity of systems and data. Although these County IT rules are not all inclusive, they provide a minimum standard that all County departments are required to adhere to.

RISKS & OPPORTUNITIES

Library's two major IT systems includes their network and the Integrated Library System, which is used to support Library operations, including the circulation and acquisition of library materials, library catalog, fines/fees accounting, customer account management, and access to online reference databases. Library has 87 locations and reported over 1,300 staff and 8,600 IT devices, such as desktops, laptops, and tablets. It is critical that Library management ensure appropriate security measures are in place to protect its systems, devices, and data.

SCOPE EXCLUSIONS

Our review was limited to an evaluation of the design of the internal controls system over Library's IT and security processes noted in the Scope and Objectives section above. While our review included tests to confirm the existence of controls (e.g., interviews and walkthroughs), it did not include tests to identify whether controls were consistently operating as designed or whether the Department continually complied with County policies. As noted further below, ensuring controls are

**LOS ANGELES COUNTY LIBRARY
INFORMATION TECHNOLOGY AND SECURITY REVIEW
BACKGROUND AND AUDIT SCOPE**

operating as designed and in compliance with County policies is the Department management's responsibility.

FOLLOW-UP PROCESS

The Auditor-Controller (A-C) has a follow-up process designed to provide assurance to the Board that departments are taking appropriate and timely corrective action to address audit recommendations. Within six months of the date of an audit report, departments must submit a Corrective Action Implementation Report (CAiR) detailing the corrective action taken to address all recommendations in the report. Departments must also submit documentation with the CAiR that demonstrates the corrective action taken. We will review departments reported corrective action and supporting documentation and report the results to the Board. For any recommendations not fully implemented, departments must report the status of corrective action within six months after our first follow-up report is issued.

MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROLS

As indicated in CFM Section 1.0, management of each County department is primarily responsible for designing, implementing, and maintaining a system of internal controls that provides reasonable assurance that important departmental and County objectives are being achieved. Internal controls should sustain and improve departmental performance, adapt to changing priorities and operating environments, reduce risks to acceptable levels, and support sound decision-making.

Management must monitor internal controls on an ongoing basis to ensure that any weaknesses or non-compliance are promptly identified and corrected. The A-C's role is to assist management by performing periodic assessments of the effectiveness of the department's internal control systems. These assessments complement, but do not in any way replace, management's responsibilities over internal controls.

LIMITATIONS OF INTERNAL CONTROLS

Any system of internal controls, however well designed, has limitations. As a result, internal controls provide reasonable but not absolute assurance that an organization's goals and objectives will be achieved. Some examples of limitations include errors, circumvention of controls by collusion, management override of controls, and poor judgment. In addition, there is a risk that internal controls may become inadequate due to changes in the organization, such as reduction in staffing or lapses in compliance.

SKYE PATRICK
Library Director

LA COUNTY LIBRARY

May 24, 2019

TO: Arlene Barrera
Acting, Auditor-Controller

FROM: Skye Patrick
Library Director

SUBJECT: **RESPONSE TO INFORMATION TECHNOLOGY AND SECURITY REVIEW**

We have reviewed your report of the Library's Information Technology and Security Review, and agree with your recommendations (see attached). The Library strives to adhere to County guidelines and has implemented corrective actions to address the recommendations in the report. We will continue to monitor internal controls over information technology and security, and revise applicable reporting procedures and processes to ensure our continued compliance with County guidelines.

We appreciate your staff's professional and courteous conduct during this audit. If you have any questions or require additional information, please have your staff contact Grace Reyes, Administrative Deputy II, at (562) 940-8406 or Greyes@library.lacounty.gov.

SP:GR:ss
OD:\compliance\audit-review\response

Attachment

LOS ANGELES COUNTY LIBRARY- INFORMATION TECHNOLOGY & SECURITY REVIEW DEPARTMENT ACTION PLAN/RESPONSE

ISSUE 1: ENCRYPTION AND ANTIVIRUS SOFTWARE PROTECTION	
A/C Recommendation	Library management enhance their encryption and antivirus software protection processes and controls to ensure all IT devices are encrypted and have current antivirus software.
Priority	PRIORITY 1
Agree/Disagree	Agree
Department Action Plan[1]	The Public Library will ensure to establish and improve upon full encryption with new acquired McAfee encryption software to all staff workstations. The Public Library has currently improved McAfee Anti-Virus software to all staff machines as a part of Library's PC refresh program. a. We will include checkoff list for installing AV for PC's. b. We will establish new processes upon implementing software. c. We will establish processes upon periodic review to ensure that devices are encrypted, and AV is completed.
Planned Implementation Date	August 30, 2019
Additional Information (optional)[2]	The Public Library is currently implementing AD Migration with additional software and encryption in new technology environment.

ISSUE 2: ENCRYPTION KEYS	
A/C Recommendation	Library management establish processes to ensure encryption keys are restricted to users with a business need and stored in a secure manner.
Priority	PRIORITY 2
Agree/Disagree	Agree
Department Action Plan[1]	The Public Library management will ensure and establish developing new processes to ensure encryption keys are restricted to System Administrator and Network Administrator. And, enhanced assigned administration provides efficient access to a separate server that store all encryption keys with Serial Numbers are set for each machine upon deployment.
Planned Implementation Date	October 15, 2019
Additional Information (optional)[2]	a. The Public Library network's current network security encryption key (WPA2, WPA) is stored in the router. Each workstation has a router's user name and password are on each device. Admins access the security settings where the network encryption key is stored. b. Encryption Keys will then be copied and stored to a separate server into a secure cloud file.

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

ISSUE 3: PASSWORD CONTROLS	
A/C Recommendation	Library management evaluate implementing password controls for their network and ILS.
Priority	PRIORITY 2
Agree/Disagree	Agree
Department Action Plan[1]	The Public Library management will ensure that a newer version of the Integrated Library System (ILS) COTS (customizable off the shelf) software for enterprise library management will be implemented with more complex passwords. We will also ensure that the network will have limited login attempts are set automatically New software version includes: a. We will ensure that the Third-party vendor option for single sign-on with integration of Active Directory and password would then match the ISD standard. b. We will ensure that the password complexity requirements are set and that three wrong logon attempts will be automatically set to lock out. c. We will ensure that password policy is in place to prohibit the sharing of passwords and enforce unique Active Directory passwords. The Public Library management will also ensure to apply policy maximum password is set on the network for every 90 days to enforce change password complexity.
Planned Implementation Date	September 15, 2019
Additional Information (optional)[2]	Upon the newly upgraded Hosted AD. The Public Library working with ISD to integrate hosted AD for single sign-on.

ISSUE 4: USER ACCESS IDS	
A/C Recommendation	Library management require unique user logon IDs to access their network.
Priority	PRIORITY 2
Agree/Disagree	Agree
Department Action Plan[1]	The Public Library management will ensure as a part of new implementation that third-party vendor sets single sign-on under new hosted Active Directory for unique logon ID's for Public Library network.
Planned Implementation Date	August 15, 2019
Additional Information (optional)[2]	

ISSUE 5: USER ACCESS REVIEWS	
A/C Recommendation	Library management establish a process to perform and document quarterly user access reviews.
Priority	PRIORITY 2

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

ISSUE 5: USER ACCESS REVIEWS	
Agree/Disagree	Agree
Department Action Plan[1]	The Public Library management will ensure to implement as a part of County initiative for Identity Management (IAM) to provide processes through change management for defined user access controls. a. This review will include any privilege users and/or any users with access to sensitive, confidential information. Change management of user access controls will be enforced quarterly for user access reviews. b. This review will include Privileged access management and controls (PAM) will be assigned to system and network administrators to ensure separation of duties is clearly defined when providing access to users.
Planned Implementation Date	October 15, 2019
Additional Information (optional)[2]	

ISSUE 6: IT SECURITY TRAINING	
A/C Recommendation	Library management establish processes and controls to train all employees annually on IT security and document their participation.
Priority	PRIORITY 2
Agree/Disagree	Agree
Department Action Plan[1]	Th Public Library management will ensure to enhance improved and implemented controls for training all employees on basis for security training through education with new software called, 'KnowBe4' and course content annually. a. KnowBe4 software launched with notifications to all staff on March 11, 2019. b. Course content added and deployed 9 modules to be completed by all staff. c. We will document and generate reports to provide status of all employee training.
Planned Implementation Date	April 11, 2019 – Fully implemented
Additional Information (optional)[2]	Additional training software through 'KnowBe4' was launched on April 16, 2019 to all staff. Part-time and Contract employees without an 'E or C' number emails will receive published lessons and sign AUA.

ISSUE 7: PHYSICAL SECURITY ACCESS	
A/C Recommendation	Library management establish processes to periodically review that access to restricted IT areas is appropriate.
Priority	PRIORITY 2
Agree/Disagree	Agree

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

ISSUE 7: PHYSICAL SECURITY ACCESS	
Department Action Plan[1]	The Public Library management has developed processes to periodically review with ongoing monitoring processes are in place and that access is restricted within IT areas that include: a. Key-cards audited and administered by the IT administration on quarterly basis b. Supervisor and Managers are responsible for requesting both, new Key-card access, as well as returning key-cards assigned to staff leaving c. All key-card access requests will be processed by the IT Admin in collaboration with Facilities. d. New sign-in and sign-out sheets and e-sign-in with laptop now administered e. Newly alarm code log request, key-card log request, lock keys log request and reviewed and monitored by IT Admin.
Planned Implementation Date	February 4, 2019- Fully implemented
Additional Information (optional)[2]	

ISSUE 8: ANNUAL INVENTORY RECONCILIATION	
A/C Recommendation	Library management develop processes to ensure the master IT equipment listing and the annual physical inventory counts are reconciled timely.
Priority	**PRIORITY 2**
Agree/Disagree	**Agree**
Department Action Plan[1]	The Public Library management will ensure and enhance improved documentation in developing new processes and ensure the master IT equipment list and annual physical inventory counts are reconciled in a timely manner as follows: a. We will ensure to all take the physical inventory counts and reconcile it to the master IT equipment list in a timely manner. b. We will ensure this will take place in a timely manner within appropriate time of the physical count. c. We will ensure that physical count is completed within a 2-3-month period and we have since completed the process for IT equipment controls.
Planned Implementation Date	January 29, 2019 – Fully implemented
Additional Information (optional)[2]	

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

ISSUE 9: MANAGEMENT MONITORING OF INTERNAL CONTROLS	
A/C Recommendation	Library management develop ongoing self-monitoring processes to ensure controls function as intended that include: a) Examination of process and control activities, such as a review of an adequate number of transactions on a regular basis to ensure adherence to County rules. b) Documenting the monitoring activity and retaining evidence so it can be subsequently validated. c) Elevating material exceptions to management on a timely basis to ensure awareness of relative control risk, and to ensure appropriate corrective actions are implemented.
Priority	PRIORITY 3
Agree/Disagree	Agree
Department Action Plan[1]	The Public Library management will ensure establishing the following steps to the current management monitoring processes: a. We will establish to compare McAfee software encryption reports and ensure devices are fully encrypted and establish and ensure management review and monitoring of McAfee Antivirus protection software is fully deployed to every workstation. b. We will establish and ensure network and system user access review is compliant with internal controls and Board Policy 6.101, Use of County Information Technology Resources. c. We will ensure the training for IT security awareness and education for all employees. d. We will establish and ensure all monitoring process of material exceptions are elevated to management for access reviews are compliant for Physical security access. We will establish management monitoring over the areas indicated on a quarterly basis.
Planned Implementation Date	November 15, 2019
Additional Information (optional)[2]	

ISSUE 10: UPDATED STANDARDS AND PROCEDURES	
A/C Recommendation	Library management update their written standards and procedures to adequately guide supervisors and staff in the performance of their duties for critical IT and security processes mentioned.
Priority	PRIORITY 3
Agree/Disagree	Agree

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

ISSUE 10: UPDATED STANDARDS AND PROCEDURES	
Department Action Plan[1]	The Public Library management will ensure establishing the processes noted below with updated written standards and procedures (S&P) for physical access to IT restricted areas, physical keys and keycards authorizations, logs and all newly updated desk procedures are completed. We will establish newly implemented keycard system to update as follows: a. Updated keycard system software with newly generated reports. We will establish all new updated procedures to include the following: b. Revised standards and detailed guidelines for staff to properly manage public access network and users (library system). c. Revised and updated standards and procedures for access controls and processes to monitor access to critical applications.
Planned Implementation Date	November 15, 2019
Additional Information (optional)[2]	

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

PRIORITY RANKING DEFINITIONS

Auditors use professional judgment to assign rankings to recommendations using the criteria and definitions listed below. The purpose of the rankings is to highlight the relative importance of some recommendations over others based on the likelihood of adverse impacts if corrective action is not taken and the seriousness of the adverse impact. Adverse impacts are situations that have or could potentially undermine or hinder the following:

a) The quality of services departments provide to the community,
b) The accuracy and completeness of County books, records, or reports,
c) The safeguarding of County assets,
d) The County's compliance with pertinent rules, regulations, or laws,
e) The achievement of critical programmatic objectives or program outcomes, and/or
f) The cost-effective and efficient use of resources.

Priority 1 Issues

Priority 1 issues are control weaknesses or compliance lapses that are significant enough to warrant immediate corrective action. Priority 1 recommendations may result from weaknesses in the design or absence of an essential procedure or control, or when personnel fail to adhere to the procedure or control. These may be reoccurring or one-time lapses. Issues in this category may be situations that create actual or potential hindrances to the department's ability to provide quality services to the community, and/or present significant financial, reputational, business, compliance, or safety exposures. Priority 1 recommendations require management's immediate attention and corrective action within 90 days of report issuance, or less if so directed by the Auditor-Controller or the Audit Committee.

Priority 2 Issues

Priority 2 issues are control weaknesses or compliance lapses that are of a serious nature and warrant prompt corrective action. Priority 2 recommendations may result from weaknesses in the design or absence of an essential procedure or control, or when personnel fail to adhere to the procedure or control. These may be reoccurring or one-time lapses. Issues in this category, if not corrected, typically present increasing exposure to financial losses and missed business objectives. Priority 2 recommendations require management's prompt attention and corrective action within 120 days of report issuance, or less if so directed by the Auditor-Controller or the Audit Committee.

Priority 3 Issues

Priority 3 issues are the more common and routine control weaknesses or compliance lapses that warrant timely corrective action. Priority 3 recommendations may result from weaknesses in the design or absence of a procedure or control, or when personnel fail to adhere to the procedure or control. The issues, while less serious than a higher-level category, are nevertheless important to the integrity of the department's operations and must be corrected or more serious exposures could result. Departments must implement Priority 3 recommendations within 180 days of report issuance, or less if so directed by the Auditor-Controller or the Audit Committee.