# LIVE VIRTUAL COMMITTEE MEETING

## TO VIEW VIA WEB

## TO LISTEN BY TELEPHONE

Access Code:

Enter the access code when prompted.

## TO PROVIDE PUBLIC COMMENT

**You may submit a request to speak during Public Comment or provide a written comment by emailing PublicComment@lacera.com. If you are requesting to speak, please include your contact information, agenda item, and meeting date in your request.**

**LOS ANGELES COUNTY EMPLOYEES RETIREMENT ASSOCIATION**
**300 N. LAKE AVENUE, SUITE 650, PASADENA, CA**

**Attention:** Public comment requests must be submitted via email to PublicComment@lacera.com no later than 5:00 p.m. the day before the scheduled meeting.

AGENDA

A SPECIAL MEETING OF THE AUDIT COMMITTEE

AND BOARD OF RETIREMENT AND BOARD OF INVESTMENTS*

LOS ANGELES COUNTY EMPLOYEES RETIREMENT ASSOCIATION

300 N. LAKE AVENUE, SUITE 810, PASADENA, CALIFORNIA 91101

8:00 A.M., THURSDAY, JUNE 25, 2020

This meeting will be conducted by the Audit Committee under the Governor's
Executive Order No. N-29-20.

Any person may listen by telephone to the meeting by
dialing 877-309-2074 Access Code 396-380-975 or view the meeting online at
https://attendee.gotowebinar.com/register/1005612642893384205

*The Committee may take action on any item on the agenda
and agenda items may be taken out of order.*

2020 AUDIT COMMITTEE MEMBERS
    Gina V. Sanchez, Chair
    Keith Knox, Vice Chair
    Herman B. Santos, Secretary
    Vivian H. Gray
    David Green

AUDIT COMMITTEE CONSULTANT
    Rick Wentzel

I.   CALL TO ORDER

II.  APPROVAL OF MINUTES

    A.  Approval of the Minutes of the Special Audit Committee Meeting of
        May 8, 2020

## III. PUBLIC COMMENT

(**You may submit written public comments by email to PublicComment@lacera.com. Please include the agenda number and meeting date in your correspondence. Correspondence will be made part of the official record of the meeting. Please submit your written public comments or documentation as soon as possible and up to the close of the meeting.

You may also request to address the Committee. A request to speak must be submitted via email to PublicComment@lacera.com no later than 5:00 p.m. the day before the scheduled meeting. Please include your contact information, agenda item, and meeting date so that we may contact you with information and instructions as to how to access the Committee meeting as a speaker.)

## IV. NON-CONSENT ITEMS

A. Recommendation as submitted by Richard Bendall, Chief Audit Executive and Christina Logan, Senior Internal Auditor: That the Committee approve the Revisions to Internal Audit Charter.
(Memo dated June 16, 2020)

B. Recommendation as submitted by Gina Sanchez, Chair Audit Committee: That the Committee authorize the issuance of a Request for Proposal for External Assessment of Internal Audit Recommendation Follow-Up Process. (Memo dated June 16, 2020)

C. Recommendation as submitted by Richard Bendall, Chief Audit Executive and Summy Voong, Senior Internal Auditor: That the Committee review and discuss the Mobile Device Management Controls Audit and provide the following action(s):

1. Accept and file report;

2. Instruct staff to forward report to Boards or Committees; and/or

3. Provide further instruction to staff.
(Memo dated June 16, 2020)

D. Recommendation as submitted by Richard Bendall, Chief Audit Executive and Kathryn Ton, Senior Internal Auditor: That the Committee review and discuss the Contract Management System (CMS) Audit and provide the following action(s):

1. Accept and file report;

2. Instruct staff to forward report to Boards or Committees; and/or

3. Provide further instruction to staff.
(Memo dated June 16, 2020)

IV. NON-CONSENT ITEMS (Continued)

E. Recommendation as submitted by Richard Bendall, Chief Audit Executive and Summy Voong, Senior Internal Auditor: That the Committee review and discuss the Clear Skies Penetration Test and Veracode Static Code Analysis and provide the following action(s):

1. Accept and file report;

2. Instruct staff to forward report to Boards or Committees; and/or

3. Provide further instruction to staff.
   (Memo dated June 16, 2020)

F. Recommendation, as submitted by Richard Bendall, Chief Audit Executive and Nathan Amick, Internal Auditor: That the Committee review and discuss the Audit of Foreign Payees Audit and provide the following action(s):

1. Accept and file report;

2. Instruct staff to forward report to Boards or Committees; and/or

3. Provide further instruction to staff.
   (Memo dated June 16, 2020)

V. REPORTS

A. Final Audit Plan Status Report - FYE June 30, 2020
   Richard Bendall, Chief Audit Executive
   Leisha Collins, Principal Internal Auditor
   (Memo dated June 16, 2020)

B. FYE 2021 Risk Assessment and Audit Plan Development
   Richard Bendall, Chief Audit Executive
   Leisha Collins, Principal Internal Auditor
   (Memo dated June 16, 2020)

C. Internal Audit's Quality Assurance and Improvement Program (QAIP)
   Richard Bendall, Chief Audit Executive
   Christina Logan, Senior Internal Auditor
   (Memo dated June 16, 2020)

V.   REPORTS (Continued)

   D.   Internal Audit Goals Report
        Richard Bendall, Chief Audit Executive
        Leisha Collins, Principal Internal Auditor
        (Memo dated June 16, 2020)

   E.   Recommendation Follow-Up Report
        Richard Bendall, Chief Audit Executive
        Gabriel Tafoya, Senior Internal Auditor
        (Memo dated June 16, 2020)

   F.   <span style="color:red">Attorney-Client Privilege/Confidential Memo</span>
        2016 Privacy Audit (By Alston & Bird) – June 2020 Follow Up
        Richard Bendall, Chief Audit Executive
        Kristina Sun, Senior Internal Auditor
        (Memo dated June 16, 2020)

   G.   Real Estate Manager Compliance Reviews
        Richard Bendall, Chief Audit Executive
        Kathryn Ton, Senior Internal Auditor
        (For Information Only) (Memo dated June 16, 2020)

   H.   Continuous Auditing Program (CAP)
        Richard Bendall, Chief Audit Executive
        Gabriel Tafoya, Senior Internal Auditor
        Nathan Amick, Internal Auditor
        (For Information Only) (Memo dated June 16, 2020)

   I.   Ethics Hotline Status Report
        Richard Bendall, Chief Audit Executive
        Kathryn Ton, Senior Internal Auditor
        (For Information Only) (Memo dated June 16, 2020)

VI.   CONSULTANT COMMENTS

   Rick Wentzel, Audit Committee Consultant
   (Verbal Presentation)

VII. GOOD OF THE ORDER
  (For Information Purposes Only)

VIII. ADJOURNMENT

*The Board of Retirement and Board of Investments have adopted a policy permitting any member of the Boards to attend a standing committee meeting open to the public. In the event five (5) or more members of either the Board of Retirement and/or the Board of Investments (including members appointed to the Committee) are in attendance, the meeting shall constitute a joint meeting of the Committee and the Board of Retirement and/or Board of Investments. Members of the Board of Retirement and Board of Investments who are not members of the Committee may attend and participate in a meeting of a Board Committee but may not vote on any matter discussed at the meeting. Except as set forth in the Committee's Charter, the only action the Committee may take at the meeting is approval of a recommendation to take further action at a subsequent meeting of the Board.*

*Documents subject to public disclosure that relate to an agenda item for an open session of the Board and/or Committee that are distributed less than 72 hours prior to the meeting will be available for public inspection at the time they are distributed to a majority of the members of any such Board and/or Committee at LACERA's offices at 300 N. Lake Avenue, Suite 820, Pasadena, CA 91101 during normal business hours [e.g., 8:00 a.m. to 5:00 p.m. Monday through Friday].*

***Requests for reasonable modification or accommodation of the telephone public access and Public Comments procedures stated in this agenda from individuals with disabilities, consistent with the Americans with Disabilities Act of 1990, may call the Board Offices at (626) 564-6000, Ext. 4401/4402 from 8:30 a.m. to 5:00 p.m. Monday through Friday or email PublicComment@lacera.com, but no later than 48 hours prior to the time the meeting is to commence.**

MINUTES OF THE SPECIAL MEETING OF THE AUDIT COMMITTEE OF THE

BOARD OF RETIREMENT AND BOARD OF INVESTMENTS

LOS ANGELES COUNTY EMPLOYEES RETIREMENT ASSOCIATION

300 N. LAKE AVENUE, SUITE 810, PASADENA, CA 91101

8:00 A.M., FRIDAY, MAY 8, 2020

*This meeting was conducted by teleconference pursuant to the Governor's Executive Order N-29-20. The public may attend the meeting at LACERA's offices.*

PRESENT:        Gina V. Sanchez, Chair

                Keith Knox, Vice Chair

                Herman B. Santos, Secretary

                Vivian H. Gray

                David Green

                MEMBERS AT LARGE

                Alan Bernstein

                Shawn R. Kehoe


                STAFF, ADVISORS, PARTICIPANTS

                Santos H. Kreimann, Chief Executive Officer

                Richard Bendall, Chief Audit Executive

                Steven P. Rice, Chief Counsel

                Leisha Collins, Principal Internal Auditor

                Christina Logan, Senior Internal Auditor

                Rick Wentzel, Audit Committee Consultant

I.   CALL TO ORDER

The meeting was called to order at 9:03 a.m., in the Board Room of Gateway

Plaza.

II.   APPROVAL OF THE MINUTES

A.   Approval of the Minutes of the Special Audit Committee Meeting of

March 4, 2020.

> Mr. Knox made a motion, Mr. Green seconded, to approve the minutes of the Special Audit Committee meeting of March 4, 2020.  The motion passed (roll call) with Messrs. Green, Knox, Santos and Ms. Gray and Ms. Sanchez voting yes.

III.   PUBLIC COMMENT

There were no requests from the public to speak.

IV.   NON-CONSENT ITEMS

A.   Recommendation as submitted by Richard Bendall, Chief Audit Executive and Christina Logan, Senior Internal Auditor: That the Committee: a) Provide direction to staff on the proposed revisions to the Audit Committee Charter; and b) Upon approval, recommend to the Board of Retirement and Board of Investments to adopt the revised Audit Charter. (Memo dated May 1, 2020)

> Mr. Santos made a motion, Mr. Knox seconded, to approve staff's recommendations. The motion passed (roll call) with Messrs. Green, Knox, Santos and Ms. Gray and Ms. Sanchez voting yes.

V.   NON-CONSENT ITEMS (Continued)

B. Recommendation as submitted by Richard Bendall, Chief Audit Executive and Leisha Collins, Principal Internal Auditor:  That the Committee: Consider and recommend the establishment of an Audit Reserve Fund in the amount of $500,000 to be funded from contingency monies and secure the Boards' delegated authority to access such reserve funds at the sole discretion of the Audit Committee based on a preliminary finding from existing audit activities that merit further investigation.  (Memo dated May 1, 2020)

> Mr. Knox made a motion, Mr. Santos seconded, to approve staff's recommendations including the following revisions: That the Audit Committee Reserve Funds be included with the report and provide the audit report to both boards at the May board meetings. The motion passed (roll call) with Messrs. Green, Knox, Santos and Ms. Gray and Ms. Sanchez voting yes.

C. Recommendation as submitted by Richard Bendall, Chief Audit Executive and Leisha Collins, Principal Internal Auditor:  That the Committee: a) Direct staff to terminate the current Audit Committee Consultant Agreement, effective July 1, 2020, and negotiate and enter into a new Audit Committee Consultant Agreement with Rick Wentzel, Sole Practitioner, at the same rate and terms as the current agreement with Grant Thornton, for the prior of July 1, 2020 to December 31, 2020, terminable at LACERA's convenience; and b) Direct staff to immediately initiate a Request for Proposal (RFP) to hire a new Audit Committee Consultant. (Memo dated May 1, 2020)

> Mr. Knox made a motion, Mr. Green seconded to approve staff's recommendation. The motion passed unanimously. The motion passed (roll call) with Messrs. Green, Knox, Santos and Ms. Gray and Ms. Sanchez voting yes.

VI.     ITEMS FOR STAFF REVIEW

There were no items for staff review.

VII.    GOOD OF THE ORDER

There was nothing to report during Good of the Order.

VIII.   ADJOURNMENT

There being no further business to come before the Committee, the meeting was

adjourned at 9:53 a.m.

**L CERA**

June 16, 2020

TO:           2020 Audit Committee
                 Gina V. Sanchez, Chair
                 Keith Knox, Vice Chair
                 Herman B. Santos, Secretary
                 Vivian H. Gray
                 David Green

                 Audit Committee Consultant
                 Rick Wentzel

FROM:        Richard Bendall
                 Chief Audit Executive

                 Christina Logan
                 Senior Internal Auditor

FOR:          June 25, 2020 Audit Committee Meeting

SUBJECT:    **Revisions to Internal Audit Charter**

**RECOMMENDATION:**

The Audit Committee review and approve Internal Audit's revised Charter and/or
provide staff further direction regarding the proposed revisions.

**BACKGROUND**

The Institute of Internal Auditors (IIA) requires internal audit functions to formally define
the purpose, authority, and responsibilities of the group in a charter. Executive
management and the Board must review and approve the charter. In addition, the IIA
requires a periodic review of the internal audit charter to ensure it is aligned with industry
standards and organizational changes. The Internal Audit Charter (IA Charter) was
established in 1996 and was lasted updated in November 2017.

Internal Audit has recently completed its review and updated the IA Charter (Attachment
A & B) to align with the IIA Model Internal Audit Charter 2017 (Attachment C), peer
charters, and revisions included in the proposed Audit Committee Charter(Attachment D).

Most of the changes were to align the Scope of Internal Audit Activities (Attachment A pages 5-6) with the proposed June 2020 Audit Committee Charter. The revised IA Charter now clarifies IA's scope to include assessing LACERA's Values & Ethics and Organizational Governance. This clarification is also, in alignment with the scope / nature of work in the periodic self-assessment IA completed this June as part of its Quality Assurance & Improvement Program.

**CONCLUSION**

Staff recommends the Audit Committee review and approve Internal Audit's revised Charter and/or provide staff further direction regarding the proposed revisions.


RB:/cl


**Attachments:**
A: Red-line Version of Revised Internal Audit Charter
B. Clean Version of Revised Internal Audit Charter
C: IIA Model Internal Audit Charter 2017
D: Clean Version of Proposed Audit Committee Charter (June 2020)

**LACERA**
Los Angeles County Employees Retirement Association

# Internal Audit Charter

**INTERNAL AUDIT SERVICES**

~~November 2017~~June 2020

# 20~~17~~**20**

**INTERNAL AUDIT CHARTER**

# LACERA

## INTERNAL AUDIT CHARTER

### I.  PURPOSE AND MISSION
The purpose of Internal Audit is to provide independent and objective assurance services, and consulting services designed to add value and improve LACERA's operations.  The mission of Internal Audit is to enhance and protect LACERA's organizational values by providing risk-based and objective assurance, advice, and insight. Internal Audit helps the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

### II.  ROLE
The internal audit activity was ~~is~~ established by the Audit Committee.  Internal Audit's responsibilities are defined by the Audit Committee as part of the Audit Committee's oversight role.

### III.  OBJECTIVES

#### A.  Assurance Objectives
The goal of assurance services is to provide an objective examination of evidence for the purpose of providing an independent assessment to Management and the Audit Committee on governance, risk management, and control processes for LACERA. Assurance services include audits and continuous process testing to assess if the organization's assets are adequately safeguarded, operating efficiency is enhanced, and compliance is maintained with prescribed laws and LACERA policies.  Assurance services also include the independent assessment of the organization's risk awareness, reliability, and integrity of the organization's data and the achievement of LACERA's goals and objectives.

#### B.  Consulting Objectives
The objective of consulting services is to provide Management with formal assessments and advice for improving LACERA's governance, risk management, and control processes, without Internal Audit assuming Management responsibility.  Internal Audit will participate as consultants in the assessment and review of controls, policies, procedures, and systems, both manual and electronic.  In addition, opportunities for improving management controls, and LACERA's image may be identified during audits; and these will be communicated to the appropriate level of Management.

**C. Advisory Objectives**

The objective of advisory services is to provide informal advice to Management. Having Internal Audit consult at the beginning of a project, aids management in identifying and managing risks effectively, and designing adequate internal controls. Examples of advisory services include participating in various committees in an ex-officio capacity; providing routine advice on policies, establishing controls, providing training and risk management tools, and facilitating meetings.

**IV. STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING**

Internal Audit will govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' International Professional International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, *the International Standards for the Professional Practice of Internal Auditing*, and the Definition of Internal Auditing. The CAE will report periodically to executive management and the Audit Committee regarding Internal Audit's conformance to the Code of Ethics and the *Standards*.

Additionally, Internal Audit will obtain guidance from the professional standards and practices of other, relevant professional organizations, including but not limited to, the American Institute of Certified Public Accountants, the Information Systems Audit and Control Association, the Associate of Certified Fraud Examiners, and the Association of Public Pension Fund Auditors.

**V. ORGANIZATION**

The Chief Audit Executive (CAE) reports functionally to the Audit Committee of the Board of Investments and Board of Retirement, and administratively to the Chief Executive Officer. This reporting structure provides for Internal Audit's independence and objectivity as required by professional standards.

The Audit Committee's roles and responsibilities are defined in the Audit Committee Charter.

**VI. AUTHORITY**

Internal Audit, with strict accountability for confidentiality, and safeguarding of records and information, is authorized full, free, and unrestricted access to any and all of LACERA's hard copy and electronic records, data maintained within IT systems or databases, physical properties, and personnel pertinent to carrying out any engagement. All employees are requested to assist Internal Audit in fulfilling its roles and responsibilities.

The CAE will have unrestricted access to, and communicate directly with the Audit Committee and Boards, subject to the requirements of the Ralph M. Brown Act (Government Code Section 54950, et seq.).

**VII. INDEPENDENCE AND OBJECTIVITY**

Internal Audit will remain free from interference by any element in the organization, including matters of audit selection, scope, procedures, frequency, timing, or report content to permit maintenance of a necessary independent and objective mental attitude.

Internal Audit will be diligent in monitoring its own potential conflicts of interest in performing its Mission, Objectives, and Responsibility under this Charter. Where a conflict is identified, the Audit Committee will be advised and a determination will be made by the Committee as to whether to proceed and procure an independent outside auditor. Internal Auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair the Internal Auditor's judgment.

Internal Auditors will exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal Auditors will make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

The CAE will confirm to the Audit Committee, at least annually, the organizational independence of the Internal Audit division. The CAE will disclose to the Audit Committee any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

> **Commented [CL1]:** Language from IIA Model

**VIII. SCOPE OF INTERNAL AUDIT ACTIVITIES RESPONSIBILTY**

The scope of internal auditing encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of LACERA's governance, risk management, and control processes as well as the quality of performance in carrying out assigned responsibilities to achieve the organization's stated goals and objectives.

**A. LACERA's Operations**

> **Commented [CL2]:** Aligns with revised AC Charter

1. Assess that management has established processes and systems that are operating within the highest fiduciary standards and are directed toward the requirements defined in the Federal and state laws, regulations, and LACERA policies and procedures.

> **Commented [CL3]:** From CalPers charter

2. Evaluate the efficiency and effectiveness of processes and resources deployed.

> **Commented [CL4]:** Moved from below.

3. Review the reliability and integrity of financial and operational information, and the means used to identify, measure, classify, and report such information.

**B. Values & Ethics**
1. Assess LACERA's processes for promoting appropriate ethics and values within the organization.
2. Review Management's process for communicating and monitoring compliance with LACERA's Code of Ethical Conduct for all stakeholders.

**C. Organizational Governance**
1. Risk Management
   a. Assess business risks and effectiveness of mitigating control mechanisms.
   b. Assess Management's implementation and maintenance of an appropriate enterprise wide risk management process.

2. Fraud
   a. Assess LACERA's processes for preventing and detecting fraud.
   b. Oversee LACERA's Ethics Hotline process.

3. System of Internal Controls
   a. Review Management's established system of internal control to ascertain whether it is functioning as designed.

4. System of Compliance
   a. Review the effectiveness of Management's system of compliance with laws, regulations, policies, and procedures that are business critical.

**D. Other Responsibilities**
1. Evaluate the quality of performance of Professional Service Providers, including the Financial Auditor, and the degree of coordination with Internal Audit.
2. Evaluate specific operations at the request of the Audit Committee, Boards, or Management, as appropriate.

This includes:
A. Evaluating risk exposure relating to achievement of LACERA's strategic objectives. Evaluating the reliability and integrity of information and the means used to identify, measure, classify, and report such information.
B. Evaluating the systems established to ensure compliance with those policies, procedures, laws, and regulations, which could have a significant impact on LACERA.
B. Evaluating the means of safeguarding assets and, as appropriate, verifying the existence of such assets.

**Commented [CL5]:** Moved from below.

**Commented [CL6]:** From IIA Standard 2110.

**Commented [CL7]:** Aligns with revised AC Charter

**Commented [CL8]:** Aligns with Standard 2110

**Commented [CL9]:** Aligns with revised AC Charter

**Commented [CL10]:** These two were moved from the 2017 Charter.

**Commented [CL11]:** See Risk Management above

C. Evaluating the effectiveness and efficiency with which resources are employed. Evaluating operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operation or programs are being carried out as planned.

**Commented [CL12]:** See LACERA's Operations

**Commented [CL13]:** See LACERA's Operations above

D. Monitoring and evaluating governance processes.

D. Monitoring and evaluating the effectiveness of LACERA's risk management processes.

**Commented [CL14]:** See Organizational Governance above

D. Evaluating the quality of performance of external auditors and the degree of coordination with Internal Audit.

**Commented [CL15]:** See Other Responsibilities above

D. Performing assurance, consulting and, advisory services related to governance, risk management, and control processes as appropriate for LACERA.

**Commented [CL16]:** In summary above

D. Reporting periodically on Internal Audit's purpose, authority, responsibilities, and performance relative to its Audit Plan.

**Commented [CL17]:** Moved to Accountability below

D. Reporting significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by the Audit Committee or Boards.

**Commented [CL18]:** See Organizational Governance above

D. Evaluating specific operations at the request of the Audit Committee, Boards, or Management, as appropriate.

**Commented [CL19]:** See Other Responsibilities

## IX. ACCOUNTABILITY

The CAE, in the discharge of his/her duties, shall be accountable to Management and the Audit Committee to:

A. Select, train, develop, and retain a competent Internal Audit staff that collectively has the abilities, knowledge, skills, experience, and professional certifications to meet the requirements of this Charter. Report to the Audit Committee significant changes in Internal Audit personnel.

B. Annually develop a flexible audit plan using an appropriate risk-based methodology, including any risks or control concerns identified by Management, the Audit Committee, or the Boards. Submit the annual Audit Plan and significant interim changes to Executive Management and the Audit Committee for review and approval.

B.C. Annually provide a proposed budget that corresponds to the annual Audit Plan and Audit Reserve Fund.

C.D. Issue reports to Management and the Audit Committee, at the conclusion of each Internal Audit engagement. The written reports will include Management's responses, and if applicable, Management's timetable for implementing recommendations or corrective actions.

E. Establish and maintain a follow-up system to monitor the disposition of results communicated to Management and ensure Management actions have been effectively implemented or that Executive Management has accepted the risk of not taking action.

D.F. Annually provide an assessment on Management's process for communicating and monitoring compliance with LACERA's Ethical Code of Conduct for all stakeholders.

G. Annually provide an assessment on the adequacy and effectiveness of LACERA's organizational governance, including risk management, fraud, system of controls, and system of compliance. processes for controlling its activities and managing its risks in the areas set forth under the mission and scope of work.

E.H. Provide a summary of all cases reported to LACERA's Ethics Hotline reports at each Audit Committee meeting.

F.I. Report significant issues related to the processes for controlling the activities of LACERA and its affiliates, including potential improvements to those processes, and provide information concerning such issues through resolution.

G.J. Periodically provide information on the status and results of the annual audit plan and the sufficiency of department resources.

**X. QUALITY ASSURANCE AND IMPROVEMENT PROGRAM**

Internal Audit will maintain a quality assurance and improvement program that covers all aspects of the division's activities. The program will include an evaluation of the division's conformance with the Definition of Internal Auditing and the Standards, and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of Internal Audit's activity and identifies opportunities for improvement.

The CAE will communicate to Executive Management and the Audit Committee on the Internal Audit division's quality assurance and improvement program, including the results of internal assessments and external assessments which are conducted at least once every five years by a qualified, independent assessor.

**XI. APPROVAL**

This Internal Audit Charter ("IA Charter") was reviewed and adopted by the Audit Committee on June 25, 2020. This IA Charter is thereby effective this day and is hereby signed by the following persons who have authority and responsibilities under this Charter.

**APPROVED AND ADOPTED BY:**


_____    _____    _____    _____
**Chair, Audit Committee**   **Date**       **Santos H. Kreimann**       **Date**
                                            *Chief Executive Officer*


_____    _____

> **Commented [CL20]:** Aligns with revised AC Charter

**LA CERA**

_____     _____

**Richard Bendall**              **Date**
_Chief Audit Executive_

**LACERA**
Los Angeles County Employees Retirement Association

# Internal Audit Charter

**INTERNAL AUDIT SERVICES**

**June 2020**

**2020**

# LACERA

## INTERNAL AUDIT CHARTER

# INTERNAL AUDIT CHARTER

### I.  PURPOSE AND MISSION
The purpose of Internal Audit is to provide independent and objective assurance services, and consulting services designed to add value and improve LACERA's operations.  The mission of Internal Audit is to enhance and protect LACERA's organizational values by providing risk-based and objective assurance, advice, and insight. Internal Audit helps the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

### II.  ROLE
The internal audit activity was established by the Audit Committee.  Internal Audit's responsibilities are defined by the Audit Committee as part of the Audit Committee's oversight role.

### III.  OBJECTIVES
#### A.  Assurance Objectives
The goal of assurance services is to provide an objective examination of evidence for the purpose of providing an independent assessment to Management and the Audit Committee on governance, risk management, and control processes for LACERA. Assurance services include audits and continuous process testing to assess if the organization's assets are adequately safeguarded, operating efficiency is enhanced, and compliance is maintained with prescribed laws and LACERA policies.  Assurance services also include the independent assessment of the organization's risk awareness, reliability, and integrity of the organization's data and the achievement of LACERA's goals and objectives.

#### B.  Consulting Objectives
The objective of consulting services is to provide Management with formal assessments and advice for improving LACERA's governance, risk management, and control processes, without Internal Audit assuming Management responsibility.   Internal Audit will participate as consultants in the assessment and review of controls, policies, procedures, and systems, both manual and electronic.  In addition, opportunities for improving management controls, and LACERA's image may be identified during audits; and these will be communicated to the appropriate level of Management.

#### C. Advisory Objectives
The objective of advisory services is to provide informal advice to Management.  Having Internal Audit consult at the beginning of a project, aids management in identifying and managing risks effectively, and designing adequate internal controls.  Examples of advisory services include participating in various committees in an ex-officio capacity;

providing routine advice on policies, establishing controls, providing training and risk management tools, and facilitating meetings.

## IV. STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING

Internal Audit will govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' International Professional International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, *the International Standards for the Professional Practice of Internal Auditing*, and the Definition of Internal Auditing.  The CAE will report periodically to executive management and the Audit Committee regarding Internal Audit's conformance to the Code of Ethics and the *Standards*.

Additionally, Internal Audit will obtain guidance from the professional standards and practices of other, relevant professional organizations, including but not limited to, the American Institute of Certified Public Accountants, the Information Systems Audit and Control Association, the Associate of Certified Fraud Examiners, and the Association of Public Pension Fund Auditors.

## V. ORGANIZATION

The Chief Audit Executive (CAE) reports functionally to the Audit Committee of the Board of Investments and Board of Retirement, and administratively to the Chief Executive Officer. This reporting structure provides for Internal Audit's independence and objectivity as required by professional standards.

The Audit Committee's roles and responsibilities are defined in the Audit Committee Charter.

## VI. AUTHORITY

Internal Audit, with strict accountability for confidentiality, and safeguarding of records and information, is authorized full, free, and unrestricted access to any and all of LACERA's hard copy and electronic records, data maintained within IT systems or databases, physical properties, and personnel pertinent to carrying out any engagement.  All employees are requested to assist Internal Audit in fulfilling its roles and responsibilities.

The CAE will have unrestricted access to, and communicate directly with the Audit Committee and Boards, subject to the requirements of the Ralph M. Brown Act (Government Code Section 54950, et seq.).

## VII. INDEPENDENCE AND OBJECTIVITY

Internal Audit will remain free from interference by any element in the organization, including matters of audit selection, scope, procedures, frequency, timing, or report content to permit maintenance of a necessary independent and objective mental attitude.

**LACERA**

Internal Audit will be diligent in monitoring its own potential conflicts of interest in performing its Mission, Objectives, and Responsibility under this Charter. Where a conflict is identified, the Audit Committee will be advised, and a determination will be made by the Committee as to whether to proceed and procure an independent outside auditor. Internal Auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair the Internal Auditor's judgment.

Internal Auditors will exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal Auditors will make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

The CAE will confirm to the Audit Committee, at least annually, the organizational independence of the Internal Audit division. The CAE will disclose to the Audit Committee any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

## VIII. SCOPE OF INTERNAL AUDIT ACTIVITIES

The scope of internal auditing encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of LACERA's governance, risk management, and control processes as well as the quality of performance in carrying out assigned responsibilities to achieve the organization's stated goals and objectives.

### A. LACERA's Operations

1. Assess that management has established processes and systems that are operating within the highest fiduciary standards and are directed toward the requirements defined in the Federal and state laws, regulations, and LACERA policies and procedures.

2. Evaluate the efficiency and effectiveness of processes and resources deployed.

3. Review the reliability and integrity of financial and operational information, and the means used to identify, measure, classify, and report such information.

### B. Values & Ethics

1. Assess LACERA's processes for promoting appropriate ethics and values within the organization.

2. Review Management's process for communicating and monitoring compliance with LACERA's Code of Ethical Conduct for all stakeholders.

**C. Organizational Governance**

1. Risk Management

   a. Assess business risks and effectiveness of mitigating control mechanisms.

   b. Assess Management's implementation and maintenance of an appropriate enterprise wide risk management process.

2. Fraud

   a. Assess LACERA's processes for preventing and detecting fraud.

   b. Oversee LACERA's Ethics Hotline process.

3. System of Internal Controls

   a. Review Management's established system of internal control to ascertain whether it is functioning as designed.

4. System of Compliance

   a. Review the effectiveness of Management's system of compliance with laws, regulations, policies, and procedures that are business critical.

**D. Other Responsibilities**

1. Evaluate the quality of performance of Professional Service Providers, including the Financial Auditor, and the degree of coordination with Internal Audit.

2. Evaluate specific operations at the request of the Audit Committee, Boards, or Management, as appropriate.

## IX. ACCOUNTABILITY

The CAE, in the discharge of his/her duties, shall be accountable to Management and the Audit Committee to:

A. Select, train, develop, and retain a competent Internal Audit staff that collectively has the abilities, knowledge, skills, experience, and professional certifications to meet the requirements of this Charter. Report to the Audit Committee significant changes in Internal Audit personnel.

B. Annually develop a flexible audit plan using an appropriate risk-based methodology, including any risks or control concerns identified by Management, the Audit Committee, or the Boards. Submit the annual Audit Plan and significant interim changes to Executive Management and the Audit Committee for review and approval.

C. Annually provide a proposed budget that corresponds to the annual Audit Plan and Audit Reserve Fund.

D. Issue reports to Management and the Audit Committee, at the conclusion of each Internal Audit engagement. The written reports will include Management's responses, and if applicable, Management's timetable for implementing recommendations or corrective actions.

E. Establish and maintain a follow-up system to monitor the disposition of results communicated to Management and ensure Management actions have been effectively implemented or that Executive Management has accepted the risk of not taking action.

F. Annually provide an assessment on Management's process for communicating and monitoring compliance with LACERA's Ethical Code of Conduct for all stakeholders.

G. Annually provide an assessment on the adequacy and effectiveness of LACERA's organizational governance, including risk management, fraud, system of controls, and system of compliance.

H. Provide a summary of all cases reported to the Ethics Hotline at each Audit Committee meeting.

I. Report significant issues related to the processes for controlling the activities of LACERA and its affiliates, including potential improvements to those processes, and provide information concerning such issues through resolution.

J. Periodically provide information on the status and results of the annual audit plan and the sufficiency of department resources.


## X. QUALITY ASSURANCE AND IMPROVEMENT PROGRAM

Internal Audit will maintain a quality assurance and improvement program that covers all aspects of the division's activities. The program will include an evaluation of the division's conformance with the Definition of Internal Auditing and the Standards, and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of Internal Audit's activity and identifies opportunities for improvement.

The CAE will communicate to Executive Management and the Audit Committee on the Internal Audit division's quality assurance and improvement program, including the results of internal assessments and external assessments which are conducted at least once every five years by a qualified, independent assessor.

## XI.  APPROVAL

This Internal Audit Charter ("IA Charter") was reviewed and adopted by the Audit Committee on June 25, 2020. This IA Charter is thereby effective this day and is hereby signed by the following persons who have authority and responsibilities under this Charter.

**APPROVED AND ADOPTED BY:**

| | | | |
|---|---|---|---|
| **Gina Sanchez** | **Date** | **Santos H. Kreimann** | **Date** |
| *Chair, Audit Committee* | | *Chief Executive Officer* | |

**Richard Bendall**          **Date**
*Chief Audit Executive*

# Supplemental Guidance

## Model Internal Audit Activity Charter

The Model Internal Audit Activity Charter is designed to illustrate common practices typically set out in an internal audit activity charter. The generic nature of this draft is intended to encourage customization.

The document may not reflect all legal or regulatory requirements that exist in the every jurisdiction. Additionally, stakeholder expectations may influence the inclusion or deletion of certain practices.

In drafting an internal audit activity charter, the chief audit executive should exercise care to customize the charter, including replacing bracketed, blue text with language that accurately reflects the user's situation.

## Purpose and Mission

The purpose of [name of organization]'s internal audit [department/activity] is to provide independent, objective assurance and consulting services designed to add value and improve [name of organization]'s operations. The mission of internal audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. The internal audit [department/activity] helps [name of organization] accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

## Standards for the Professional Practice of Internal Auditing

The internal audit [department/activity] will govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *International Standards for the Professional Practice of Internal Auditing*, and the Definition of Internal Auditing. The chief audit executive will report periodically to senior management and the [board/audit committee/supervisory committee] regarding the internal audit [department/activity]'s conformance to the Code of Ethics and the *Standards*.

## Authority

The chief audit executive will report functionally to the [board/audit committee/supervisory committee] and administratively (i.e., day-to-day operations) to the [chief executive officer].To establish, maintain, and assure that [name of organization]'s internal audit [department/activity] has sufficient authority to fulfill its duties, the [board/audit committee/supervisory committee] will:

- Approve the internal audit [department/activity]'s charter.
- Approve the risk-based internal audit plan.
- Approve the internal audit [department/activity]'s budget and resource plan.
- Receive communications from the chief audit executive on the internal audit [department/activity]'s performance relative to its plan and other matters.
- Approve decisions regarding the appointment and removal of the chief audit executive.
- Approve the remuneration of the chief audit executive.
- Make appropriate inquiries of management and the chief audit executive to determine whether there is inappropriate scope or resource limitations.

The chief audit executive will have unrestricted access to, and communicate and interact directly with, the [board/audit committee/supervisory committee], including in private meetings without management present.

The [board/audit committee/supervisory committee] authorizes the internal audit [department/activity] to:

- Have full, free, and unrestricted access to all functions, records, property, and personnel pertinent to carrying out any engagement, subject to accountability for confidentiality and safeguarding of records and information.
- Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports.
- Obtain assistance from the necessary personnel of [name of organization], as well as other specialized services from within or outside [name of organization], in order to complete the engagement.

## Independence and Objectivity

The chief audit executive will ensure that the internal audit [department/activity] remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If the chief audit executive determines that independence or objectivity may be impaired in fact or appearance, the details of impairment will be disclosed to appropriate parties.

Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises are made, and that they do not subordinate their judgment on audit matters to others.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair their judgment, including:

- Assessing specific operations for which they had responsibility within the previous year.
- Performing any operational duties for [name of organization] or its affiliates.
- Initiating or approving transactions external to the internal audit [activity/department].

- Directing the activities of any [name of organization] employee not employed by the internal audit [department/activity], except to the extent that such employees have been appropriately assigned to auditing teams or to otherwise assist internal auditors.

Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards will be established to limit impairments to independence or objectivity.

Internal auditors will:

- Disclose any impairment of independence or objectivity, in fact or appearance, to appropriate parties.
- Exhibit professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined.
- Make balanced assessments of all available and relevant facts and circumstances.
- Take necessary precautions to avoid being unduly influenced by their own interests or by others in forming judgments.

The chief audit executive will confirm to the [board/audit committee/supervisory committee], at least annually, the organizational independence of the internal audit [department/activity].

The chief audit executive will disclose to the [board/audit committee/supervisory committee] any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

## Scope of Internal Audit Activities

The scope of internal audit activities encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments to the [board/audit committee/supervisory committee], management, and outside parties on the adequacy and effectiveness of governance, risk management, and control processes for [name of organization]. Internal audit assessments include evaluating whether:

- Risks relating to the achievement of [name of organization]'s strategic objectives are appropriately identified and managed.
- The actions of [name of organization]'s officers, directors, employees, and contractors are in compliance with [name of organization]'s policies, procedures, and applicable laws, regulations, and governance standards.
- The results of operations or programs are consistent with established goals and objectives.

- Operations or programs are being carried out effectively and efficiently.
- Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact [name of organization].
- Information and the means used to identify, measure, analyze, classify, and report such information are reliable and have integrity.
- Resources and assets are acquired economically, used efficiently, and protected adequately.

The chief audit executive will report periodically to senior management and the [board/audit committee/supervisory committee] regarding:

- The internal audit [department/activity]'s purpose, authority, and responsibility.
- The internal audit [department/activity]'s plan and performance relative to its plan.
- The internal audit [department/activity]'s conformance with The IIA's Code of Ethics and *Standards,* and action plans to address any significant conformance issues.
- Significant risk exposures and control issues, including fraud risks, governance issues, and other matters requiring the attention of, or requested by, the [board/audit committee/supervisory committee].
- Results of audit engagements or other activities.
- Resource requirements.
- Any response to risk by management that may be unacceptable to [name of organization].

The chief audit executive also coordinates activities, where possible, and considers relying upon the work of other internal and external assurance and consulting service providers as needed. The internal audit [department/activity] may perform advisory and related client service activities, the nature and scope of which will be agreed with the client, provided the internal audit [department/activity] does not assume management responsibility.

Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during engagements. These opportunities will be communicated to the appropriate level of management.

## Responsibility

The chief audit executive has the responsibility to:

- Submit, at least annually, to senior management and the [board/audit committee/supervisory committee] a risk-based internal audit plan for review and approval.

- Communicate to senior management and the [board/audit committee/supervisory committee] the impact of resource limitations on the internal audit plan.
- Review and adjust the internal audit plan, as necessary, in response to changes in [name of organization]'s business, risks, operations, programs, systems, and controls.
- Communicate to senior management and the [board/audit committee/supervisory committee] any significant interim changes to the internal audit plan.
- Ensure each engagement of the internal audit plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.
- Follow up on engagement findings and corrective actions, and report periodically to senior management and the [board/audit committee/supervisory committee] any corrective actions not effectively implemented.
- Ensure the principles of integrity, objectivity, confidentiality, and competency are applied and upheld.
- Ensure the internal audit [department/activity] collectively possesses or obtains the knowledge, skills, and other competencies needed to meet the requirements of the internal audit charter.
- Ensure trends and emerging issues that could impact [name of organization] are considered and communicated to senior management and the [board/audit committee/supervisory committee] as appropriate.
- Ensure emerging trends and successful practices in internal auditing are considered.
- Establish and ensure adherence to policies and procedures designed to guide the internal audit [department/activity].
- Ensure adherence to [name of organization]'s relevant policies and procedures, unless such policies and procedures conflict with the internal audit charter. Any such conflicts will be resolved or otherwise communicated to senior management and the [board/audit committee/supervisory committee].
- Ensure conformance of the internal audit [department/activity] with the *Standards*, with the following qualifications:
    o If the internal audit [department/activity] is prohibited by law or regulation from conformance with certain parts of the *Standards*, the chief audit executive will ensure appropriate disclosures and will ensure conformance with all other parts of the *Standards*.
    o If the *Standards* are used in conjunction with requirements issued by [other authoritative bodies], the chief audit executive will ensure that the internal audit [department/activity] conforms with the *Standards*, even if the internal audit [department/activity] also conforms with the more restrictive requirements of [other authoritative bodies].

## Quality Assurance and Improvement Program

The internal audit [department/activity] will maintain a quality assurance and improvement program that covers all aspects of the internal audit [department/activity]. The program will include an evaluation of the internal audit [department/activity]'s conformance with the *Standards* and an evaluation of whether internal auditors apply The IIA's Code of Ethics. The program will also assess the efficiency and effectiveness of the internal audit [department/activity] and identify opportunities for improvement.

The chief audit executive will communicate to senior management and the [board/audit committee/supervisory committee] on the internal audit [department/activity]'s quality assurance and improvement program, including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside [name of organization].

## Approval/Signatures

_____            _____

Chief Audit Executive                                                    Date


_____            _____

[Board/Audit Committee/Supervisory Committee] Chair        Date


_____            _____

[Chief Executive Officer]                                                Date

## About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

## About Supplemental Guidance

Supplemental Guidance is part of The IIA's International Professional Practices Framework (IPPF) and provides additional recommended (nonmandatory) guidance for conducting internal audit activities. While supporting the *International Standards for the Professional Practice of Internal Auditing*, Supplemental Guidance is not intended to directly link to achievement of conformance with the *Standards*. It is intended instead to address topical areas, as well as sector-specific issues, and it includes detailed processes and procedures. This guidance is endorsed by The IIA through formal review and approval processes.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance or www.theiia.org/guidance.

## Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance material is not intended to provide definitive answers to specific individual circumstances and, as such, is only intended to be used as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

## Copyright

March 17

**L CERA**
Los Angeles County Employees Retirement Association

# Audit Committee Charter

# June 2020

**2020**

# LACERA

## AUDIT COMMITTEE CHARTER

**Table of Contents**

# AUDIT COMMITTEE CHARTER

## I. CHARTER

This Charter establishes the authority and responsibilities of the Audit Committee, as assigned by Los Angeles County Employees Retirement Association's (LACERA) Board of Retirement and Board of Investments (Boards). The Audit Committee Charter is a living document and should be reviewed at least every three years.

## II. PURPOSE AND ASSIGNED FIDUCIARY OVERSIGHT DUTIES

In November 2003, LACERA's Boards established the LACERA Audit Committee.

The purpose of the Audit Committee is to assist the Boards in fulfilling their fiduciary oversight duties for the:

   A. Internal Audit Activity
   B. Professional Service Provider Activity
   C. Financial Reporting Process
   D. Values and Ethics, and
   E. Organizational Governance

## III. PRINCIPLES OF THE AUDIT COMMITTEE

The Audit Committee will conduct itself in accordance with LACERA's Code of Ethical Conduct and the following core principles from the Institute of Internal Auditors' (IIA) Code of Ethics. The Audit Committee expects the Boards, Management, and staff will also adhere to these requirements.

**Integrity –** The Audit Committee Members will perform their work with honesty, diligence, and responsibility. The Audit Committee expects and will encourage transparency when fulfilling its duties. Communications between Committee Members, Management, staff, and/or Professional Service Providers will be open, direct, and complete. Subject to applicable laws and organizational limitations, Internal Audit will regularly provide the Audit Committee with updates on audit and consulting projects completed and related findings and follow-up.

**Independence & Objectivity -** The Audit Committee will perform its responsibilities in an independent manner and in compliance with fiduciary duty without exception. Audit Committee Members will disclose any conflicts of interest (actual or perceived) to the Committee.

**Confidentiality** – The Audit Committee Members will be prudent in the use and protection of information acquired during the course of its duties.

**Competency** - Audit Committee Members will receive formal orientation training on the purpose and mandate of the Committee and LACERA's objectives. Audit Committee Members are obligated to prepare for and participate in Committee meetings.

**Professional Standards -** The Audit Committee will ensure all related work will be handled with the highest professional standards consistent with auditing standards of practice and industry guidelines.

## IV. AUTHORITY

The Audit Committee will have unrestricted access to Management and staff, and any relevant information it considers necessary to discharge its duties. All employees are directed to cooperate with the Committee and its requests. If access to requested information is denied due to legal or confidentiality reasons, the Audit Committee and/or CAE will follow a prescribed, Board approved mechanism for resolution of the matter.

The Audit Committee has the authority to conduct or authorize investigations into any matters within its scope of duties, including engaging independent counsel and/or other advisors it deems necessary.

The Audit Committee is empowered to:
1. Approve the appointment, compensation, and work of the Financial Auditor hired to audit LACERA's financial statements.

2. Approve the appointment, compensation, and work of other Professional Service Providers to perform non-financial statement audits, reviews, or investigations, subject to limitations due to confidentiality, legal standards, and/or where approval will clearly impair the purpose or methods of the audit.

3. Resolve any significant disagreements regarding risks, findings, and/or payment between Management and the Financial and/or Other Service Providers.

## V. AUDIT COMMITTEE COMPOSITION AND CONSULTANT

The Audit Committee will consist of the chair and vice-chair of the Boards of Retirement and Investments, plus one additional Board member elected annually by each Board, for a total of four to six members[1]. Board chairs and vice-chairs that leave Board service will be replaced automatically on the Audit Committee when the Board replaces its missing officer while other Committee membership remains intact. If any elected Audit Committee member leaves Board service or resigns from the Audit Committee prior to the completion of their term, the Board of the departing member, will elect a new Audit Committee member at the next

---

[1] The number of Committee members is dependent upon the designated Chair and Vice Chair appointments to the Boards of Retirement and Investments. If both Boards were to elect the same individuals to the positions of Chair and/or Vice Chair, the Audit Committee would be comprised of four or five Board Members.

regularly scheduled Board meeting.  If Audit Committee voting results in a tie, the Committee will forward the recommendation to the appropriate Board for consideration and final decision.

The Committee shall have the authority to approve the hiring of the Audit Committee Consultant as an advisor through a Request for Proposal process. The Audit Committee Consultant will be designated as the audit technical and financial expert, to advise the Committee on audit and financial matters. The Audit Committee Consultant's contract will be for three years.

At the first Committee meeting of each calendar year, the Committee shall elect a Chairman, Vice Chair and Secretary, each to serve for a term of one year or until his or her successor is duly elected and qualified, whichever is less. In the event of a vacancy in the office of chair, the vice chair shall immediately assume the office of chair for the remainder of the term. In the event of a vacancy in the office of vice chair or secretary, the Committee shall elect one of its members to fill such vacancy for the remainder of the term, at its next regular meeting.

## VI.  AUDIT COMMITTEE MEETINGS

The Audit Committee will conduct regular meetings at least four times per year, with authority to convene additional meetings, as circumstances require.  The time frame between Audit Committee meetings should not exceed four months.

All Committee Members are expected to attend each meeting.

Regular meeting notices and agendas will be posted at least 72 hours in advance of the regular meetings and will be made available to the public in accordance with the Ralph M. Brown Act (Government Code Sections 54950, et seq.). Public documents referred to in the agenda will be made available for review at the office of the staff secretary to the Committee. The Committee will invite members of Management, Internal Auditors, Financial Auditors, all other Professional Service Providers, and/or others to attend meetings and provide pertinent information, as necessary.

Special meetings of the Committee may be called in the manner provided by Government Code Section 54956(a).  The Committee will have such other powers as provided in the Brown Act.

Robert's Rules of Order, except as otherwise provided herein, shall guide the Committee in its proceedings; however, the chair of the Committee shall have the same rights to vote and participate in discussions as any other member of the Committee without relinquishing the chair. The order of business shall be as determined by formal action of the Committee. Four members of a six-member Audit Committee or three members of a four or five-member Audit Committee, excluding the audit consultant, constitute a quorum.

The secretary of the Committee shall cause to be recorded in the minutes the time and place of each meeting of the Committee, the names of the members present, all official acts of the Committee, the votes given by members except when the action is unanimous, and when requested by a member, that member's dissent or approval with his or her reasons, and shall cause the minutes to be written forthwith and presented for approval at the next regular meeting.

## VII. RESPONSIBILITIES

### A. Internal Audit Activity

1. Internal Audit Strategy and Annual Plan

    a. Review and provide input on Internal Audit's annual risk assessment

    b. Review and approve Internal Audit's Annual Audit Plan (Plan) and resource plan, make recommendations concerning audit projects.

    c. Recommend to the Boards a budget to achieve the Plan plus a contingent budget for additional work related to audit findings or other unplanned work.

    d. Review and monitor Internal Audit's activity relative to its Plan. Review and approve all major changes to the Plan.

2. Internal Audit Engagement & Follow-Up

    a. Review and discuss engagement reports to take the following action(s):

        i. accept and file report,

        ii. instruct staff to forward report to Boards or Committees,

        iii. make recommendations to the Boards or Committees regarding actions as may be required based on audit findings and/or,

        iv. provide further instruction to staff.

    b. Monitor Internal Audit's recommendations to ensure Management has adequately and timely addressed the risk(s) identified, either through implementing a new policy, procedure, or process, or accepting the associated risk.

    c. Inquire whether any evidence of fraud has been identified during internal or external audit engagements, and evaluate what additional actions, if any, should be taken.

    d. Inquire whether any audit or non-audit engagements have been completed but not reported to the Audit Committee; if so, inquire whether any matters of significance arose from such work.

    e. Review and advise Management and the Boards on the results of any special investigations.

3. Standards Conformance

    a. Approve the Internal Audit Charter.

    b. Ensure the Internal Audit Division conforms with the IIA's International Standards for the Professional Practice of Internal Audit, particularly the independence of Internal Audit and its organizational structure.

    c. Ensure the Internal Audit Division has a quality assurance and improvement program (QAIP), and that the results of these periodic assessments are presented to the Audit Committee.

    d. Ensure the Internal Audit Division has an external quality assurance review every five years. Review the results of the external quality assurance review and monitor the implementation of related recommendations.

      Advise the Boards about any recommendations for the continuous improvement of the internal audit activity.

4. Chief Audit Executive (CAE)

Since the CAE reports to the Chief Executive Officer (CEO) for administrative purposes, but to the Audit Committee for functional purposes, the Audit Committee will be responsible for the following:

    a. Make recommendations to both Boards regarding the appointment, discipline, dismissal, and/or removal of the CAE, which will be addressed by the Boards in a joint meeting. Both Boards will make the final decisions as to the appointment, discipline, dismissal, and/or removal of the CAE. The CEO has authority to administer minor discipline, which is limited to counseling memos and written warnings, with notice of such discipline to be provided to the Committee and the Boards at their next meetings. Consideration by the Boards and the Committee concerning the appointment, discipline, dismissal, and/ or removal of the CAE will be made in executive session under Government Code Section 54957(b).

    b. Perform the CAE's annual assessment with qualitative input from the CAE and CEO. The Committee's discussion regarding the CAE's annual performance evaluation will be made in executive session under Government Code Section 54957(b).

    c. Administer the CAE's annual salary adjustment using the Boards' established compensation structure.

**B. Professional Service Provider Activity**

The Audit Committee is responsible for the oversight of all work performed by professional service providers (Service Providers) for audits, reviews, or investigations, including the audit of LACERA's financial statements.

1. Approve the appointment and compensation of the External Financial Auditor, hired to perform an independent audit of LACERA's financial statements. Oversee the work of the Financial Auditor, including review of the Financial Auditor's proposed audit scope and approach, as well as coordination with Internal Audit and Management.

2. Approve the appointment and compensation of other Professional Service Providers, hired to perform non-financial statement audits, reviews or consulting, subject to limitations due to confidentiality, legal standards, and/or where approval will clearly impair the purpose or methods of the audit.

3. Review the Professional Service Providers, including the Financial Auditor, and Management the results of the work performed, any findings and recommendations, Management's responses, and actions taken to implement the audit recommendations.

## C. Financial Reporting Process

The Audit Committee is responsible for the oversight of the independent audit of LACERA's financial statement, including but not limited to overseeing the resolution of audit findings in areas such as internal control, legal, regulatory compliance, and ethics.

1. Review significant accounting and reporting issues, including complex or unusual transactions and highly judgmental areas, recent professional and regulatory pronouncements, and understand their impact on the financial statements.

2. Review with Management and the Financial Auditors the results of the audit, including any difficulties encountered.

3. Review the annual financial statements, consider whether they are complete, consistent with information known to Committee members, and reflect appropriate accounting principles.

4. Review with Management and the Financial Auditors all matters required to be communicated to the Committee under *Generally Accepted Auditing Standards*.

## D. Values and Ethics

1. Review and assess LACERA's Code of Ethical Conduct established by the Boards and Management.

2. Annually, review Management's process for communicating LACERA's Code of Ethical Conduct to Trustees, Management, and staff, and for monitoring compliance therewith.

3. Review reports received relating to conflicts of interest and ethics issues, and if appropriate, make a recommendation to the Boards.

**E. Organizational Governance**
To obtain reasonable assurance with respect to LACERA's governance process, the Audit Committee will review and provide advice on the governance process established and maintained, and the procedures in place to ensure they are operating as intended.

1. Risk Management

   a. Annually review LACERA's risk profile.

   b. Obtain from the CAE an annual report on Management's implementation and maintenance of an appropriate enterprise wide risk management process. Provide advice on the risk management processes established and maintained, and the procedures in place to ensure that they are operating as intended.

   c. Provide oversight on significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by Management and the Boards.

2. Fraud

   a. Oversee Management's arrangements for the prevention and detection of fraud, including ensuring adequate time is spent discussing and raising awareness about fraud and the Hotline.

   b. Review a summary of Hotline reports, and if appropriate make a recommendation to the Boards.

3. System of Internal Controls

   a. Consider the effectiveness of LACERA's internal control system, including information technology security and control, as well as all other aspects of LACERA's operations.

   b. Understand the scope of Internal and External Auditors' review of internal control over financial reporting, and obtain reports on significant findings and recommendations, together with Management's responses.

   c. Review and provide advice on control of LACERA as a whole and its individual divisions.

4. System of Compliance

   a. Annually, review the effectiveness of Management's system of compliance with laws, regulations, policies, and procedures that are business critical.

  b. As needed, review the observations and findings of any examinations by regulatory agencies.

  c. Obtain regular updates from Management and LACERA's Legal Office regarding compliance matters.

  d. At least annually, review reported activity to ensure issues of fraud, noncompliance, and/or inappropriate activities are being addressed.

**F. Other Responsibilities**

1. Report to the Boards as needed about the Audit Committee's activities, issues, and related recommendations.

2. Provide an open avenue of communication between Internal Audit, all Professional Service Providers, including the Financial Auditor, Management, and the Boards.

3. Perform other activities related to this Charter as requested by the Boards.

4. Review and assess the adequacy of the Committee's Charter at least every three years, requesting the Boards' approval for proposed changes.

**VIII. APPROVAL**

This Charter was reviewed by the Audit Committee on May 8, 2020 and approved by the Board of Investments and Board of Retirement on June 24, 2020. This Charter is thereby effective June 24, 2020 and is hereby signed by the following persons who have authority and responsibilities under this Charter.

 

**Gina Sanchez**         **Date**
*Chair, Audit Committee*

 

**David Green**          **Date**
*Chair, Board of Investments*

 

**Herman Santos**         **Date**
*Chair, Board of Retirement*

# LACERA

June 16, 2020

TO:         2020 Audit Committee
              Gina V. Sanchez, Chair
              Keith Knox, Vice Chair
              Herman B. Santos, Secretary
              Vivian H. Gray
              David Green

              Audit Committee Consultant
                Rick Wentzel

FROM:       Gina V. Sanchez
              Chair, Audit Committee

FOR:        June 25, 2020 Audit Committee Meeting

SUBJECT:    External Assessment of Internal Audit Recommendation Follow-Up Process

## RECOMMENDATION

**That the Audit Committee authorize an external quality assessment to evaluate the Internal Audit Division's recommendation follow-up process for compliance with the *International Standards for the Professional Practice of Internal Auditing* (Standards) and Code of Ethics issued by the Institute of Internal Auditors (IIA). The assessment will be overseen on a day-to-day basis on behalf of the Committee by its Chair, with the assistance of LACERA's Chief Executive Officer and Chief Counsel.  A vendor with the required minimum qualifications stated in the Standards and IIA's Implementation Guide will be brought to the Committee for approval before the assessment begins.**

## DISCUSSION

*A.  The IIA Standards for Recommendation Follow-Up and External Assessment*

Under the Standards, the Chief Audit Executive must establish and maintain a follow-up process to monitor and ensure that recommendations have been effectively implemented or that senior management has accepted the risk of not taking action.  The required follow-up process is a central activity of Internal Audit in evaluating the adequacy, effectiveness, and timeliness of management's response to audit recommendations, including those made by Internal Audit itself as well as by external auditors and others.   The Implementation Guide for the Standards states that a compliant follow-up process typically includes:

1. Observations communicated to management and their relative risk rating.
2. The nature of the agreed corrective actions.
3. The timing, guidelines, and age of the corrective actions and changes in target dates.
4. The management or process owner responsible for each corrective action.
5. The current status of corrective actions, and whether Internal Audit has confirmed the status.

The Implementation Guide refers to use of a tool, mechanism, or system, such as a spreadsheet or database, to track, monitor, and report on such information. It is expected that information in the tracking system will be updated periodically and that the Chief Audit Executive will inquire of management on a set frequency, such as quarterly, as to the status of corrective actions. The Chief Audit Executive may also choose to confirm corrective actions through a future audit. The Implementation Guide states that reporting is determined based on the Chief Audit Executive's judgment and agreed expectations, and can have different forms and elements, including observations, risk rating and ranking, and statistics, such as percentage of corrective actions on track, overdue, and completed on time. As a leading practice, reporting should capture and measure positive improvement based on the execution of corrective actions.

The Standards recognize the importance of internal and external assessments as part of quality assurance and improvement for the internal audit function. The Chief Audit Executive must develop and maintain a Quality Assurance and Improvement Program (QAIP). The Standards require that an external assessment of the Internal Audit program be conducted at least once every five years to determination conformance with the Standards and the IIA's Code of Ethics. The external assessment report should include: the scope and frequency of the assessment; the qualifications and independence of the assessment team, including any potential conflicts of interest; the conclusions of the assessors; and corrective action plans.

Interpretation contained in the Standards state that a qualified external assessment team shall have the following minimum qualifications:

1. Demonstrate competence in the professional practice of internal auditing and the external assessment process. Competence can be demonstrated through a combination of years of experience and theoretical learning. Experience in similar organizations is more valuable than less relevant experience. The competencies of an assessment team are judged based on the team as a whole.
2. Independence, in that the assessment team does not have either an actual or potential conflict of interest and is not part of or under the control of the organization to which the internal audit activity belongs.

The IIA's Implementation Guide for external assessments recommends the following additional preferred qualifications:

1. That the team include a competent certified internal audit professional.
2. Current in-depth knowledge of the IIA's International Professional Practices Framework (IPPF) for the Standards.
3. Knowledge of leading internal auditing practices.
4. At least three years of recent experience in internal auditing at a management level that demonstrates a working knowledge and application of the IPPF.
5. That the assessment team leader have:
   a. An additional level of competence and experience from previous external quality assessment work and/or completion of the IIA's quality assessment training or similar training.
   b. Chief audit executive or comparable senior internal audit management experience.
   c. Relevant technical expertise and industry experience, which in the case of this project would specifically include the recommendation follow-up process and pension, governmental, benefits, and/or financial experience.

### B. LACERA's Practice

At LACERA, the Chief Audit Executive maintains a recommendation follow-up process under the Standards, and presents periodic reports to the Audit Committee. The follow-up process and the reporting format provided to the Committee have changed over time, including recent revisions intended to improve the process.

The Chief Audit Executive arranges for a periodic external peer review of the entire internal audit activity in compliance with the external assessment requirement of the Standards and Internal Audit's QAIP. The peer review includes the recommendation follow-up process, as part of overall divisional operations. Under the Internal Audit Charter, the peer review shall be conducted every five years. The last peer review was completed January 15, 2016. Internal Audit intends to arrange for a peer review in fiscal year 2020-2021. In the past, separate review of specific internal audit activities, such as the recommendation follow-up process, has not been conducted, but rather such review has been part of the overall divisional peer review.

### C. The Audit Committee's Oversight

Under its Charter, the Audit Committee has a fiduciary oversight responsibility to oversee LACERA's internal audit function. The Committee ensures that the Internal Audit Division complies with IIA Standards. The Charter provides that the Committee shall monitor Internal Audit's recommendations and the effectiveness of the recommendation follow-up process. The Committee is required by the Charter to ensure that the Internal Audit Division has a QAIP, and that the results are presented to the Committee.

In its oversight of the Internal Audit Division, the Audit Committee is not limited to reliance upon the peer review process overseen by the division.  Under the Charter, the Committee may select external consultants to conduct audits, reviews, or investigations, without limitation as to subject matter.

### D. External Assessment of Internal Audit's Recommendation Follow-Up Process

Given the core importance of the recommendation follow-up process to the effectiveness of Internal Audit, it is reasonable for the Audit Committee to conduct an external assessment of that process for compliance with the IIA's Standards and Code of Ethics separate from the peer review.  The assessment should be conducted as soon as possible so that findings may be reviewed by the Committee and any necessary changes made.  The assessment should be conducted by the Committee, separate from Internal Audit and outside of Internal Audit's supervision and oversight, to ensure independence and avoid the appearance of conflicts.

The assessment team should have both the minimum and preferred qualifications stated in the Interpretation to the IIA Standards and the IIA's Implementation Guide, as set forth in Section A of the Discussion above.

It is recommended that the assessment be conducted with the day-to-day oversight, as needed, of the Audit Committee Chair to provide guidance, Committee-level perspective, and assistance.  At the staff level, the Chief Executive Officer and Chief Counsel will manage the assessment and assist the selected vendor.  This approach is needed to improve independence by placing oversight of the external assessment in the hands of the Committee.  The first task of this group will be to solicit proposals for the scope of work and present a vendor for approval by the Committee before work begins.  The cost of the assessment is proposed to be charged against Internal Audit's budget for external audits.

c:      Santos H. Kreimann
        Jonathan Grabel
        Steven P. Rice
        Richard Bendall
        JJ Popowich

# LACERA

June 16, 2020

TO:       2020 Audit Committee
              Gina V. Sanchez, Chair
              Keith Knox, Vice Chair
              Herman B. Santos, Secretary
              Vivian H. Gray
              David Green

              Audit Committee Consultant
              Rick Wentzel

FROM:    Richard Bendall
            Chief Audit Executive

            Summy Voong
            Senior Internal Auditor

FOR:     June 25, 2020 Audit Committee Meeting

SUBJECT:  **Mobile Device Management (MDM) Controls Audit**

**RECOMMENDATION**

**In accordance with the current Audit Committee Charter, staff recommends that the Audit Committee review and discuss the following engagement report to take the following action(s):**

1. **accept and file report and/or,**
2. **instruct staff to forward report to Boards or Committees and/or,**
3. **provide further instruction to staff.**

**ENGAGEMENT REPORTS**

a. Mobile Device Management (MDM) Controls Audit
   Summy Voong, Senior Internal Auditor
   (Report issued: June 4, 2020)

Attachments

SV

**LACERA INTERNAL AUDIT DIVISION**

**MOBILE DEVICE MANAGEMENT CONTROLS AUDIT**

June 4, 2020

**AUDIT PERFORMED BY:**
Summy Voong, CISA, CISM
*Senior Internal Auditor*

## AUDIT REPORT

| | |
|---|---|
| **Audit Name:** | Mobile Device Management Controls Audit |
| **Responsible Division:** | Systems Division |
| **Audit Rating***: | Unsatisfactory |
| **Prior Audit Rating*:** | N/A |
| **Prior Report Date:** | N/A |

## BACKGROUND

As the result of issues noted in the November 2019 Los Angeles County Auditor-Controller's audit of LACERA's administrative operations, we added a Mobile Device Management Controls audit to the Fiscal Year (FY) 2019 – 2020 audit plan. Mobile devices provide staff and Trustees access to data and applications previously restricted to a physical location. However, the same features that make mobile devices desirable and lend to greater productivity also make them a security challenge. For example, the portable nature of these devices makes them vulnerable to loss or theft and according to recent statistics, mobile devices are under increasing attack by cyber-criminals. This can expose LACERA to additional risks, such as device theft, malicious software, and potential disclosure of sensitive information on the device.

Mobile Device Management (MDM) is a term for the administration of mobile devices in the workplace. MDM can include security and management software used to monitor and manage mobile devices across various service providers (e.g., Verizon, AT&T or T-Mobile) and operating systems (e.g., iOS, Android or Windows). LACERA internally manages its mobile devices using two different third-party MDM software applications, one specific for smartphones and tablets (IBM MaaS360) and another for laptops (Microsoft Intune). Regardless of the software used, both tools allow LACERA to centrally manage each type of device from a single unified console. MaaS360 and Intune deploy configuration settings to devices during enrollment that define requirements and restrictions, such as encryption and access passcodes. Maas360 also has the ability to continuously monitor enrolled devices for security compliance, remotely locate and lock a device if necessary, remotely remove data from lost or stolen devices, and apply profiles that limit incorrect passcode attempts before removing all data on the device.

The Systems Division has historically been responsible for all aspects of mobile device management related to cellular phones and tablets, including approval, purchasing, configuration, inventory, tracking, and disposal. The Administrative Services Division is responsible for purchasing and tracking all other LACERA assets, including laptops, and maintaining the Fixed Assets Register. In addition to the mobile devices hardware, Systems is also responsible for managing the cellular data lines for each device. Staff and Trustees issued a LACERA device must observe and comply with specific acceptable usage guidelines and must acknowledge their responsibilities by agreeing to the *LACERA Issued Mobile Device Guideline* or *iPad Usage Policy*. As of calendar year ending December 31, 2019, LACERA had approximately 270 mobile devices, with an associated annual expenditure of approximately $93,000. Almost 140 of the mobile devices consist of laptops, notebooks, and netbooks while approximately 130 consists of smartphones, tablets, and wireless hotspots.

---

* See Appendix 1 for Audit Rating

## AUDIT OBJECTIVE AND SCOPE

The objectives of the audit were to:

1. Assess the adequacy of LACERA's mobile device management program.
2. Evaluate the design and effectiveness of internal controls over administration of mobile devices and wireless service charges to ensure:
   a. Mobile devices are appropriately approved, purchased, inventoried, reconciled, monitored, and deactivated/disposed
   b. Monthly wireless service charges are appropriately reviewed for usage, overages and excessive costs
3. Determine if mobile device security controls and procedures conform with industry standards and best practices to mitigate unauthorized access to confidential or sensitive member information.
4. Determine compliance with established LACERA mobile device management, acceptable usage and procurement policies.

The scope of the audit covered the period from November 1, 2018 through December 31, 2019 and included the following devices:

- Smartphones
- Laptops, notebooks, netbooks and tablets
- Portable digital assistants (PDAs)
- Portable Universal Serial Bus (USB) devices for storage (such as thumb drives) and for connectivity (such as Wi-Fi and Bluetooth)
- Radio frequency identification (RFID) and mobile RFID (M-RFID) devices for data storage, identification, and asset management

This audit was performed in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

## AUDIT RATING AND SUMMARY OF FINDINGS

In our opinion, operational procedures and controls over mobile device management are **Unsatisfactory**. The System's Division should significantly strengthen mobile device management oversight and controls by:

1. Developing a comprehensive and consolidated mobile device management policy.
2. Ensuring appropriate internal controls exist over the procurement of mobile devices.
3. Finalizing a complete mobile device inventory.
4. Registering LACERA issued mobile devices to the mobile device management (MDM) tools.
5. Defining organizational baseline MDM usage and security configurations.
6. Defining a mobile device equipment standard that documents the business purpose by classification of recipients and a separate procedure for test devices.
7. Improving administration over mobile device acknowledgement and usage forms.
8. Actively monitoring and reconciling mobile device usage and wireless service costs.
9. Strengthening mobile device deactivation, reassignment, and disposal procedures.
10. Strengthening administrative controls over restricting universal serial bus (USB) enabled workstations.

Each of the above Findings are detailed in the following pages, including our Recommendations and Management Action Plans.

We would like to thank the Systems and Administrative Services Divisions for their cooperation with this audit.

**REVIEWED AND APPROVED**

_____    **Date:** June 4, 2020

Richard Bendall
*Chief Audit Executive*

**REPORT DISTRIBUTION**

| | | |
|---|---|---|
| 2020 Audit Committee | Santos H. Kreimann, CEO | James P. Brekk, Systems Division Manager |
| Rick Wentzel, Audit Committee Consultant | J.J. Popowich, AEO | Kimberly Hines, Administrative Services Division Manager |
| | Steven Rice, Chief Legal Counsel | Internal Audit Group |

## FINDING #1

| Develop a comprehensive and consolidated mobile device management policy | Risk Rating** |
|---|---|
| | **High** |

### OBSERVATION

Based on our review, LACERA currently has four (4) separate mobile device policies, created at various times over the last 10 years with three (3) designated for staff (one iPad Policy and two versions of a cell phone policy) and one (1) general mobile device policy specifically for Trustees. After reviewing the policies, we determined the policies were incomplete and outdated and although they defined acceptable usage, monthly allowances, and end users' responsibilities, they did not include the following:

- Type of information or devices permitted to access organizational information including standards and criteria for mobile device security, issuance, and management. Without defining these criteria's, the organization may not be limiting its risks by permitting the most-controlled devices to have the most access and the least-controlled devices to have only minimal access.
- Guidelines and standards defining the authorization, purchasing, maintenance, inventory process, and disposing of mobile devices. This will ensure staff applies approved and consistent procedures while managing mobile devices.

### RISK

Without a comprehensive mobile device management policy, the organization's expectations are not clearly defined. Clear policies are critical to effective enterprise risk management. Documentation of policies and procedures improve the effectiveness and efficiency of compliance efforts and unlock opportunities to improve business processes.

### RECOMMENDATIONS:

1. Systems Division management should develop a comprehensive and consolidated organizational mobile device management policy to be approved by the Executive Office. The policy should include the following:
   - Data classification or information security standards that govern the level of security settings configured on each device.
   - Device monitoring requirements that includes regular assessments of mobile devices for excessive, personal, reimbursable or exception usage.
   - Documented cost control monitoring and follow-up.
   - Device issuance, specification, configuration and returns standards that align with business need criteria and job-related duties and functions.

---

** See Appendix 2 for Finding's Risk Rating

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by September 30, 2020. The Systems Division created a draft W*ireless Policy and Procedures* document in February 2020 in response to the LA County audit.  The finalization of the policy and procedures has been delayed as the result of the COVID-19 pandemic; however, Systems will review that policy and include items from this recommendation.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

September 30, 2020

## FINDING #2

| Ensure appropriate internal controls exist over procurement of mobile devices | Risk Rating[**] |
| --- | --- |
| | Low |

## OBSERVATION

LACERA's *Policy for Purchasing Goods and Services* (Procurement Policy) states that the centralized procurement unit in Administrative Services is the Purchasing Agent for LACERA. We noted during testing that although laptops were purchased by Administrative Services, the Systems Division historically purchased mobile phones and tablets directly from the wireless carrier. Systems management indicated this was the policy established by the Executive Office and Administrative Services, preceding 2018, due to the technical nature of the products. Systems Division management stated as of October 2019, mobile phone and tablets are purchased through the Administrative Services Division in accordance with the Procurement Policy.

As part of our detailed testing, we obtained a listing of all devices purchased during the audit scope period from November 1, 2018 through December 31, 2019 which identified three (3) cell phones in October 2019. We determined the procurement of the three cell phones purchased for testing purposes were made through Procurement. The only variance from the Policy was that Systems took delivery of all three devices directly from the carrier, which is not the standard receiving process. Administrative Services generally takes delivery of all goods for recording in Great Plains and asset tagging. For these three phones, Internal Audit confirmed that although Systems took delivery of the items, Administrative Services coordinated later with Systems to attach an asset tag to the device paperwork and registered them in Great Plains.

---

[**] See Appendix 2 for Finding's Risk Rating

## RISK

Without adherence to the Procurement Policy for the purchase of mobile devices, including their receipt and recording in inventory by Administrative Services, proper segregation of duties and internal controls over procurement of mobile devices is weakened and there is an increased risk of erroneous or unauthorized transactions.

## RECOMMENDATIONS:

2. Systems Division and Administrative Services Division management ensure mobile devices are purchased and received in compliance with the LACERA Procurement Policy and recorded by Administrative Services in Great Plains inventory prior to being delivered to the Systems Division.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and both Administrative Services and the Systems Division assert that this recommendation has been implemented. All mobile device purchases by the Systems Division are made through Procurement in compliance with the Procurement Policy.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Administrative Services Division Management

## TARGET COMPLETION DATE

Completed.

## FINDING #3

| Finalize a complete mobile device inventory | Risk Rating[**] |
|---|---|
| | High |

## OBSERVATION

LACERA has over 270 mobile devices, approximately 180 of which are equipped with a cellular data line. The devices consist of 140 laptops, notebooks or netbooks, and 130 smartphones, tablets, and wireless hotspots. Administrative Services registers all laptops, notebooks, and netbooks in the Great Plains Fixed Asset Register. However, prior to October 2019, mobile phones and tablets were not recorded or tracked in Great Plains per prior Executive Office direction. Systems internally tracked those assets separately using excel spreadsheets. As part of our testing, we requested all mobile device inventory listings from Systems which consisted of 1) wireless cellular lines, 2) smartphones and tablets registered to MaaS360, and 3) laptops registered to Microsoft Intune.

Per review of the wireless cellular lines and comparison to the MDM listings, we noted Systems had not completed a physical inventory, including spare, vacant, or test devices. Our review further identified areas to strengthen segregation of duties and controls around the mobile device inventory process. Specifically,

---

[**] See Appendix 2 for Finding's Risk Rating

mobile phones and tablets should be recorded and tracked in Great Plains, which represent an independent inventory list for validation against Systems internal records. Systems should also work in conjunction with Administrative Services to consistently perform an inventory of mobile devices including old, spare, obsolete and test devices.

## RISK

Without a complete and accurate list of active and inactive devices as well as an independent inventory register, LACERA may be susceptible to misappropriation or loss, lack of accountability for the deployment and use of devices, and increased costs.

## RECOMMENDATIONS:

3a. Systems Division management create a current mobile device master listing that includes all active, inactive, vacant, and test devices issued by LACERA. Systems work with Administrative Services to record all mobile devices in Great Plains.

3b. Administrative Services and Systems management develop and implement a control-based mobile device inventory process. The process should include:

- Require execution of a formalized and documented annual inventory that includes active, inactive, vacant, and test devices.
- Documented responsibility for mobile device inventory asset accountability and tracking, device master listing maintenance, asset reconciliations and verification counts.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendations and plans to complete implementation by December 31, 2020. The Systems Division plans to continue maintaining the mobile device master listing outside of Great Plains to ensure appropriate recording of device information such as inactive, vacant, and test statuses. However, Systems will work with Administrative Services to ensure changes to the master listing are timely updated in Great Plains by Administrative Services.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Administrative Services Division Management

## TARGET COMPLETION DATE

December 31, 2020

## FINDING #4

| Register LACERA issued mobile devices to the mobile device management (MDM) tools | Risk Rating** |
|---|---|
| | **Medium** |

### OBSERVATION

As previously stated, LACERA has over 270 mobile devices of which 180 are equipped with a cellular data line. Our comparison of the wireless cellular lines to the MDM devices listings found that LACERA does not register all organization issued mobile devices to the respective MDM tools. Specifically, we noted approximately 20 mobile phones or tablets were not registered to MaaS360, and only 21 of 138 laptops were registered to Intune. Systems management stated it was a business decision and for technical logistics to not register all devices such as unassigned spare mobile phones or test devices used by Systems. In some cases, it is also not technically possible to register not-yet deployed or configured devices in MDM. Systems further stated most of the other, typically older 117 laptops have hardware or software that are incompatible with Intune and expect future laptop purchases to meet those specifications.

### RISK

Mobile devices that have been deployed for production use but not registered to the MDM tools could be out of compliance with LACERA's MDM security policies and may be vulnerable to data leakage or unauthorized access.

### RECOMMENDATIONS:

4. Systems Division management define the organizational mobile device management (MDM) registration policy to be approved by the Executive Office. This should include documented exceptions to the policy, if any, approved by the Executive Office.

### MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by October 31, 2020. Systems Division management will work with the Executive Office to define the appropriate organizational MDM registration policy for all devices including spare or test devices.

### RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

### TARGET COMPLETION DATE

October 31, 2020

---

** See Appendix 2 for Finding's Risk Rating

## FINDING #5

| Define organizational baseline mobile device management (MDM) usage and security configurations | Risk Rating[**] |
|---|---|
| | Medium |

### OBSERVATION

A mobile device baseline security configuration is a documented set of minimum specifications intended to prevent unauthorized use of mobile apps or device features vulnerable to cyber threats. Organizations commonly restrict users from performing certain functions on their assigned mobile devices to appropriately secure organizational devices and data. We observed that Systems does have six (6) different security configurations in the IBM MaaS360 tool; for example, a unique configuration for Board iPads, staff iPads, staff iPhones vs. test iPhones, etc. Generally, Systems Division management is also focused on security and while they may have created these configurations with specific intent, it was not defined and documented.

Further, we compared the settings against LACERA's *Unsafe Computer Practices Policy*, Federal standards as defined by the National Institute of Standards and Technology (NIST), and industry best practices. Our analysis determined that functions were not restricted within the various configurations to ensure compliance with LACERA's *Unsafe Computer Practices Policy*. For example, although the Policy prohibits users from installing mobile apps without Systems Division knowledge and consent, the Systems Division, per direction by the Executive Office preceding 2016, did not limit that functionality for end-users through the MDM tool.

### RISK

LACERA may not be limiting its cyber security risks by ensuring device settings or features are appropriately restricted. This can leave a device exposed to vulnerabilities and weaknesses that cyber criminals could exploit.

### RECOMMENDATIONS:

5a. Systems management in conjunction with the Executive Office define organizational baseline mobile device management (MDM) usage and security configurations to strengthen device security. This should include limiting or restricting any high-risk functions with documented exceptions to the policy.
5b. Establish periodic review of policy settings to ensure they remain current with industry standards and best practices.

### MANAGEMENT'S ACTION PLAN

Management agrees with these recommendations and plans to complete implementation by October 31, 2020. The Systems Division evaluates security considerations in all implementation decisions and will work with the Executive Office to ensure appropriate operations objectives are met during this process.

---

[**] See Appendix 2 for Finding's Risk Rating

**RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN**

Systems Division Management
Executive Office

**TARGET COMPLETION DATE**

October 31, 2020

**FINDING #6**

| Define a mobile device equipment standard that documents the business purpose by classification of recipients and a separate procedure for test devices | Risk Rating[**] |
|---|---|
| | **High** |

**OBSERVATION**

In about 2012, LACERA adopted a standard of using and deploying Apple devices for mobile use. However, we noted that this was an informal decision by the Executive Office that was not documented.

Based on our analysis of System's wireless cellular list, we determined there were also sixteen (16) Android devices assigned to Systems staff and one Trustee in addition to their Apple devices. Systems management stated it was not the intention to include Android devices for mass deployment and those devices served testing and long-term evaluation purposes. However, we noted again that testing of these devices was informal without any documented purpose, plan or reporting of results, and was done without any formal Executive Office approval. In addition, we noted managers and staff are typically assigned between one and three mobile devices, those being a laptop, iPad and/or phone. However, we noted Systems Division management and or staff having up to 11 mobile devices each, including multiple phones and multiple tablets.

We verified six (6) individuals in the Systems Division were assigned more than one test device of the same type (e.g., two iPads) and often with the same wireless carrier and for an undetermined and extended period of time. Systems Division management stated it was common for staff to evaluate multiple test devices of the same brand but different models on the same wireless carrier to evaluate the different model's functionality with the carrier. However, we identified two instances where test devices of identical brand and model were used for testing on the same wireless carrier. In one instance by the same individual doing the testing. While testing of devices does not necessarily require wireless usage, we noted that these devices were all connected to wireless lines in calendar year 2019, but many of them had very minimal and virtually no or actually zero wireless usage in some cases.

Further, we noted Trustees typically receive an iPad and a laptop. We determined, however, one Trustee had 5 mobile devices including two tablets, one of them a Samsung android tablet test device, two laptops, and an active wireless hotspot still assigned to them but related to a previously returned laptop.

---

[**] See Appendix 2 for Finding's Risk Rating

## RISK

Undocumented exceptions to organizational standards and policies regarding the deployment and use of mobile devices weakens the effectiveness of those standards and policies and could result in, at a minimum, the appearance of waste, fraud, and abuse.

## RECOMMENDATIONS:

6a. Systems Division Management should formalize and obtain Executive Office approval of mobile device issuance standards for staff and trustees and any exceptions to those standards should be documented and approved by the Executive Office.

6b. Systems Division Management should formalize and obtain Executive Office approval of a procedure for testing mobile devices.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendations and plans to complete implementation by October 31, 2020. The Systems Division will work with the Executive Office to define the mobile device issuance standards for staff, trustees, and test mobile devices.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

October 31, 2020

## FINDING #7

| Improve administration over mobile device acknowledgement and usage forms | Risk Rating[**] |
|---|---|
| | High |

## OBSERVATION

As previously stated, there are currently four (4) separate mobile device policies, which are incomplete and outdated. The staff policies include an area for signature/user acknowledgment, but we determined it was not obtained in practice. Alternatively, the Systems Division maintains a separate *Property Designation Form* for end users to sign when taking possession of the device.

Systems provided the signed Property Designations Forms for our audit testing as evidence that users acknowledge and abide by LACERA's mobile device policies. We noted that the form only contains acknowledgment of the quantity and type of devices issued and does not include acknowledgement that the user has read and will abide by LACERA's policies. Further, we determined that these acknowledgements

---

[**] See Appendix 2 for Finding's Risk Rating

are only obtained the first time a person receives a mobile device. No further acknowledgment was obtained either annually or when a similar device was replaced for the same user.

## RISK

Without current user acknowledgement forms, the organization may not be holding users accountable to their responsibilities, acceptable behavior, and usage restrictions of LACERA devices.

## RECOMMENDATIONS:

7. Systems Division management should improve the administrative process over mobile device acknowledgement and usage forms. The process should include the following:
    - Inclusion of the Form in the comprehensive and consolidated Mobile Device Management Policy.
    - Requirement that staff and Trustees re-sign a mobile device acknowledgement form annually and whenever provided a new device.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by October 31, 2020.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management

## TARGET COMPLETION DATE

October 31, 2020

## FINDING #8

| Actively monitor and reconcile mobile device usage and wireless service costs | Risk Rating[**] |
|---|---|
| | High |

## OBSERVATION

As part of our testing, we analyzed all wireless bills for 2019 and noted the organization had an average of 189 wireless service lines, of which approximately 87 or 46% had limited or zero usage. Specifically, 15 wireless lines had usage fewer than 30 minutes and 72 had zero usage during 2019. Further, we noted 40 of the 87 limited or zero usage lines (46%) were designated as vacant or belonged to former staff or Trustees.

Systems staff verified that vacant lines are held to reserve the cellular number for LACERA's future use. Systems management also confirmed that some wireless lines were reassigned to current staff and some limited or zero usage devices serve a valid business purpose such as Disaster Recovery or Business Continuity. However, we noted only five reassigned lines in our testing of the 87 vacant lines reflected in

---

[**] See Appendix 2 for Finding's Risk Rating

the charts below, which summarize the devices usage and service costs for 2019. We also noted in December 2019, LACERA disconnected 61 of the vacant wireless lines as a result of the LA County Audit and those costs were eliminated.

**Zero Usage**

| Device Type | # of Devices | Annual Costs |
|---|---|---|
| Tablets | 28 | $ 8,812 |
| Laptops/Aircards | 32 | $ 7,623 |
| Cellphones | 7 | $ 3,661 |
| Smartphones | 5 | $ 1,884 |
| **Totals** | **72** | **$ 21,980** |

**Limited Use\***

| Device Type | # of Devices | Annual Costs |
|---|---|---|
| Smartphones | 5 | $ 3,018 |
| Tablets | 9 | $ 2,151 |
| Laptops/Aircards | 1 | $ 232 |
| **Totals** | **15** | **$ 5,401** |

\* Less 30 minutes, 3 GB, or 36 Text Messages

In addition to limited or zero usage devices, we also reviewed the wireless bills for abnormal charges. Our review of the August 2019 billing cycle specifically identified abnormal international data roaming charges were incurred totaling $5,875. Appropriate documentation validating the costs and Executive Office approval for the additional charges was not retained.

### RISK

Inadequate mobile device monitoring exposes the organization to additional costs, inefficient usage management, and could result in waste, fraud and abuse or the appearance of it.

### RECOMMENDATIONS:

8.  Systems Division management establish guidelines approved by the Executive Office over the management and monitoring of wireless lines.

### MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by September 30, 2020. The Systems Division has performed a reconciliation of wireless service lines in March 2020 to enhance documentation of some zero and limited usage lines as standby, backup, quick availability, and those maintained for legal holds. The finalization of further action items from the reconciliation has been delayed as the result of the COVID-19 pandemic; however, System's will complete those steps during implementation of this recommendation.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management

Executive Office

## TARGET COMPLETION DATE

September 30, 2020

## FINDING #9

| Strengthen mobile device deactivation, reassignment and disposal procedures | Risk Rating[**] |
|---|---|
| | High |

## OBSERVATION

To determine timely deactivation of wireless services and proper disposal of mobile devices, we examined the 2019 monthly wireless services bills for all carriers and inquired with staff regarding disposal procedures. We determined LACERA had approximately 40 wireless lines designated as "vacant" or belonged to former staff and Trustees. Although Systems management stated some devices were reassigned, we noted devices, some of which had belonged to staff or trustees who had left LACERA service up to five (5) ago, were still not reassigned. Further, we identified the following disposal procedures that required improvement:

- LACERA has not disposed of any old or obsolete tablets or smartphones since inception of the mobile device program.
- Formal documentation to validate that old or obsolete and devices returned by staff were appropriately reset to factory settings or the data was wiped is not maintained.
- A former Trustee's iPad is still considered outstanding according to the most recent Trustee inventory count performed by the Board Offices in December 2019.
- Former Trustees could purchase their LACERA issued iPad. However, documentation outlining the approval and process was not maintained.

## RISK

Wireless services not disconnected timely could lead to unnecessary service charges. Inadequate reassignment and disposal of devices expose them to prolonged risks of misuse, theft or loss.

## RECOMMENDATIONS:

9. Systems Division management develop a formal procedure approved by the Executive Office over the deactivation, reassignment, disposal and/or sale of mobile devices taken out of service. Additionally, this procedure should include the following:
   - A timeframe and methodology for the disposal of devices.

---

[**] See Appendix 2 for Finding's Risk Rating

- Formal documentation to validate that old, obsolete devices are appropriately reset to factory settings and wiped with a copy provided to the end user and Administrative Services.
- An accurate inventory of out of service devices is maintained.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by October 31, 2020.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

October 31, 2020

## FINDING #10

| Strengthen administrative controls over restricting universal serial bus (USB) enabled workstations | Risk Rating[**] |
|---|---|
| | Medium |

## OBSERVATION

Per inquiry with Systems staff, Internal Audit noted the default LACERA workstation configuration enables USB access on all workstations. Systems then deploys a separate Group Policy Object (GPO), which is a collection of systems administrator settings that disables USB access to individual workstations. This process indicates that Systems must maintain a deny USB GPO list of 498 workstations. We noted a more effective approach would be to change the default setting to disable USB access during configuration and deploy a GPO that enables USB access. This will reduce the USB GPO listing to only approved workstations and assist Systems with performing a periodic review of approved workstations. Further, we found that there is no requirement or process to ensure that only encrypted USB devices are used for LACERA business.

## RISK

Inefficient controls over USB enabled workstations increases the risk of unauthorized transfer and removal of confidential LACERA information resulting in potential privacy incidents or breaches.

## RECOMMENDATIONS:

10. Systems Division management strengthen the process for managing workstations that have USB access enabled. The process should include:
    - A periodic review of USB enabled workstations to ensure such access is still appropriate.
    - A periodic reconciliation of the deny USB access listing against Administrative Services Fixed Asset Register.

---

[**] See Appendix 2 for Finding's Risk Rating

- Encryption required for USB devices connected to LACERA workstations.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by October 31, 2020.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management

## TARGET COMPLETION DATE

October 31, 2020

<div align="center">

**APPENDIX 1**

**AUDIT RATING SCALE**
</div>

Internal Audit issues three standard audit report evaluations as defined below:

### Satisfactory

The control environment is acceptable with minor issues having been identified. The overall environment contains sufficient internal controls to address key risks, and business practices generally comply with Company policies. Corrective action should be implemented to address any weaknesses identified during the audit in order to maintain or enhance the control environment.

### Opportunities for Improvement

The control environment has opportunities for improvement with significant issues, individually or in the aggregate, having been identified or major noncompliance with Company policies. The overall environment contains insufficient internal controls to address key risks. Prompt corrective action should be implemented to address the weaknesses and strengthen the control environment.

### Unsatisfactory

The control environment is unacceptable with critical issues, individually or in the aggregate, having been identified or major noncompliance with Company policies. The overall environment contains insufficient internal controls to address key risks and the impact may be substantial in size or nature or their effect cannot be quantified. Immediate corrective action should be implemented to address the weaknesses and strengthen the control environment.

## APPENDIX 2
## FINDING'S RISK RATING SCALE

Findings identified during the course of the audit are assigned a risk rating, as outlined in the table below. The risk rating is based on the financial, operational, compliance, or reputational impact that the issue identified could have on LACERA.

| Rating | Financial | Internal Controls | Compliance | Reputational | Executive Management |
|---|---|---|---|---|---|
| **High** | Large financial impact to LACERA or members<br><br>Actions not aligned with fiduciary responsibilities | Missing or inadequate key internal controls<br><br>Not adequate to identify fraud, noncompliance or misappropriation | Noncompliance with applicable Federal or state laws or LACERA's policies | High probability for external audit issues and/or negative public perception | Important critical business process identified by Exec Office<br><br>Requires immediate attention |
| **Medium** | Moderate financial risk to LACERA or members<br><br>Actions could be better aligned with fiduciary responsibilities | Partial key internal controls<br><br>Not adequate to identify noncompliance or misappropriation in timely manner | Inconsistent compliance with applicable Federal or state laws or LACERA's policies | Potential for external audit issues and/or negative public perception | Relatively important<br><br>May or may not require immediate attention |
| **Low** | Low financial impact to LACERA or members<br><br>Actions generally aligned with fiduciary responsibilities | Internal controls in place but not consistently efficient/effective<br><br>Implementing / enhancing controls could prevent future problems | General compliance with applicable Federal or state laws or LACERA's policies, but some minor discrepancies exist | Low probability for external audit issues and/or negative public perception | Lower significance<br><br>Does not require immediate attention |

**LACERA INTERNAL AUDIT DIVISION**

**MOBILE DEVICE MANAGEMENT CONTROLS AUDIT**

**Version with Audit Committee Comments & Internal Audit Responses**

June 4, 2020

**AUDIT PERFORMED BY:**
Summy Voong, CISA, CISM
*Senior Internal Auditor*

## AUDIT REPORT

| Audit Name: | Mobile Device Management Controls Audit |
|---|---|
| Responsible Division: | Systems Division |
| Audit Rating*: | Unsatisfactory |
| Prior Audit Rating*: | N/A |
| Prior Report Date: | N/A |

## BACKGROUND

As the result of issues noted in the November 2019 Los Angeles County Auditor-Controller's audit of LACERA's administrative operations, we added a Mobile Device Management Controls audit to the Fiscal Year (FY) 2019 – 2020 audit plan. Mobile devices provide staff and Trustees access to data and applications previously restricted to a physical location. However, the same features that make mobile devices desirable and lend to greater productivity also make them a security challenge. For example, the portable nature of these devices makes them vulnerable to loss or theft and according to recent statistics, mobile devices are under increasing attack by cyber-criminals. This can expose LACERA to additional risks, such as device theft, malicious software, and potential disclosure of sensitive information on the device.

Mobile Device Management (MDM) is a term for the administration of mobile devices in the workplace. MDM can include security and management software used to monitor and manage mobile devices across various service providers (e.g., Verizon, AT&T or T-Mobile) and operating systems (e.g., iOS, Android or Windows). LACERA internally manages its mobile devices using two different third-party MDM software applications, one specific for smartphones and tablets (IBM MaaS360) and another for laptops (Microsoft Intune). Regardless of the software used, both tools allow LACERA to centrally manage each type of device from a single unified console. MaaS360 and Intune deploy configuration settings to devices during enrollment that define requirements and restrictions, such as encryption and access passcodes. Maas360 also has the ability to continuously monitor enrolled devices for security compliance, remotely locate and lock a device if necessary, remotely remove data from lost or stolen devices, and apply profiles that limit incorrect passcode attempts before removing all data on the device.

The Systems Division (Systems) has historically been responsible for all aspects of mobile device management related to cellular phones and tablets, including approval, purchasing, configuration, inventory, tracking, and disposal. The Administrative Services Division is responsible for purchasing and tracking all other LACERA assets, including laptops, and maintaining the Fixed Assets Register. In addition to the mobile devices hardware, Systems is also responsible for managing the cellular data lines for each device. Staff and Trustees issued a LACERA device must observe and comply with specific acceptable usage guidelines and must acknowledge their responsibilities by agreeing to the *LACERA Issued Mobile Device Guideline* or *iPad Usage Policy*. As of calendar year ended December 31, 2019, LACERA had approximately 270 mobile devices, with an associated annual expenditure of approximately $93,000. Almost 140 of the mobile devices consist of laptops, notebooks, and netbooks while approximately 130 consists of smartphones, tablets, and wireless hotspots.

---

* See Appendix 1 for Audit Rating

## AUDIT OBJECTIVE AND SCOPE

The objectives of the audit were to:

1. Assess the adequacy of LACERA's mobile device management program.
2. Evaluate the design and effectiveness of internal controls over administration of mobile devices and wireless service charges to ensure:
   a. Mobile devices are appropriately approved, purchased, inventoried, reconciled, monitored, and deactivated/disposed
   b. Monthly wireless service charges are appropriately reviewed for usage, overages and excessive costs
3. Determine if mobile device security controls and procedures conform with industry standards and best practices to mitigate unauthorized access to confidential or sensitive member information.
4. Determine compliance with established LACERA mobile device management, acceptable usage and procurement policies.

The scope of the audit covered the period from November 1, 2018 through December 31, 2019 and included the following devices:

- Smartphones
- Laptops, notebooks, netbooks and tablets
- Portable digital assistants (PDAs)
- Portable Universal Serial Bus (USB) devices for storage (such as thumb drives) and for connectivity (such as Wi-Fi and Bluetooth)
- Radio frequency identification (RFID) and mobile RFID (M-RFID) devices for data storage, identification, and asset management

This audit was performed in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

## AUDIT RATING AND SUMMARY OF FINDINGS

In our opinion, operational procedures and controls over mobile device management are **Unsatisfactory**. The Systems Division should significantly strengthen mobile device management oversight and controls by:

1. Developing a comprehensive and consolidated mobile device management policy.
2. Ensuring appropriate internal controls exist over the procurement of mobile devices.
3. Finalizing a complete mobile device inventory.
4. Registering LACERA issued mobile devices to the mobile device management (MDM) tools.
5. Defining organizational baseline MDM usage and security configurations.
6. Defining a mobile device equipment standard that documents the business purpose by classification of recipients and a separate procedure for test devices.
7. Improving administration over mobile device acknowledgement and usage forms.
8. Actively monitoring and reconciling mobile device usage and wireless service costs.
9. Strengthening mobile device deactivation, reassignment, and disposal procedures.
10. Strengthening administrative controls over restricting universal serial bus (USB) enabled workstations.

Each of the above Findings are detailed in the following pages, including our Recommendations and Management Action Plans.

We would like to thank the Systems and Administrative Services Divisions for their cooperation with this audit.

**REVIEWED AND APPROVED**

_____     **Date:** June 4, 2020

Richard Bendall
*Chief Audit Executive*

**REPORT DISTRIBUTION**

| | | |
|---|---|---|
| 2020 Audit Committee | Santos H. Kreimann, CEO | James P. Brekk, Systems Division Manager |
| Rick Wentzel, Audit Committee Consultant | J.J. Popowich, AEO | Kimberly Hines, Administrative Services Division Manager |
| | Steven Rice, Chief Legal Counsel | Internal Audit Group |

## FINDING #1

| Develop a comprehensive and consolidated mobile device management policy | Risk Rating** |
|---|---|
| | **High** |

### OBSERVATION

Based on our audit, LACERA currently has four (4) separate mobile device policies, created at various times over the last 10 years with three (3) designated for staff (one iPad Policy and two versions of a cell phone policy) and one (1) general mobile device policy specifically for Trustees. After reviewing the policies, we determined the policies were incomplete and outdated and although they defined acceptable usage, monthly allowances, and end users' responsibilities, they did not include the following:

- Type of information or devices permitted to access organizational information including standards and criteria for mobile device security, issuance, and management. Without defining these criteria, the organization may not be limiting its risks by permitting the most-controlled devices to have the most access and the least-controlled devices to have only minimal access.
- Guidelines and standards defining the authorization, purchasing, maintenance, inventory process, and disposing of mobile devices. This will ensure staff applies approved and consistent procedures while managing mobile devices.

### RISK

Without a comprehensive mobile device management policy, the organization's expectations are not clearly defined. Clear policies are critical to effective enterprise risk management. Documentation of policies and procedures improve the effectiveness and efficiency of compliance efforts and unlock opportunities to improve business processes.

### RECOMMENDATIONS:

1. Systems Division management should develop a comprehensive and consolidated organizational mobile device management policy to be approved by the Executive Office. The policy should include the following:
   - Data classification or information security standards that govern the level of security settings configured on each device.
   - Device monitoring requirements that includes regular assessments of mobile devices for excessive, personal, reimbursable or exception usage.
   - Documented cost control monitoring and follow-up.
   - Device issuance, specification, configuration and returns standards that align with business need criteria and job-related duties and functions.

---

** See Appendix 2 for Finding's Risk Rating

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by September 30, 2020. The Systems Division created a draft W*ireless Policy and Procedures* document in February 2020 in response to the LA County audit. The finalization of the policy and procedures has been delayed as the result of the COVID-19 pandemic; however, Systems will review that policy and include items from this recommendation.

**AC Question: What LA County Audit?**
**IA Response: Los Angeles County Auditor-Controller's audit of LACERA's administrative operations completed in November 2019.**

**AC Question: Is the draft Wireless Policy and Procedures a consolidated document?**
**IA Response: Yes, this document should eventually replace the 4 separate policies.**

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

September 30, 2020

## FINDING #2

| Ensure appropriate internal controls exist over procurement of mobile devices | Risk Rating[**] |
|---|---|
| | Low |

## OBSERVATION

LACERA's *Policy for Purchasing Goods and Services* (Procurement Policy) states that the centralized procurement unit in Administrative Services is the Purchasing Agent for LACERA. We noted during testing that although laptops were purchased by Administrative Services, the Systems Division historically purchased mobile phones and tablets directly from the wireless carrier. Systems management indicated this was the policy established by the Executive Office and Administrative Services, preceding 2018, due to the technical nature of the products. Systems Division management stated as of October 2019, mobile phone and tablets are purchased through the Administrative Services Division in accordance with the Procurement Policy.

As part of our detailed testing, we obtained a listing of all devices purchased during the audit scope period from November 1, 2018 through December 31, 2019 which identified three (3) cell phones in October 2019. We determined the procurement of the three cell phones purchased for testing purposes were made through Procurement. The only variance from the Policy was that Systems took delivery of all three devices directly from the carrier, which is not the standard receiving process. Administrative Services generally takes

---

[**] See Appendix 2 for Finding's Risk Rating

delivery of all goods for recording in Great Plains and asset tagging. For these three phones, Internal Audit confirmed that although Systems took delivery of the items, Administrative Services coordinated later with Systems to attach an asset tag to the device paperwork and registered them in Great Plains.

## RISK

Without adherence to the Procurement Policy for the purchase of mobile devices, including their receipt and recording in inventory by Administrative Services, proper segregation of duties and internal controls over procurement of mobile devices is weakened and there is an increased risk of erroneous or unauthorized transactions.

## RECOMMENDATIONS:

2. Systems Division and Administrative Services Division management to ensure mobile devices are purchased and received in compliance with the LACERA Procurement Policy and recorded by Administrative Services in Great Plains inventory prior to being delivered to the Systems Division.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and both Administrative Services and the Systems Division assert that this recommendation has been implemented. All mobile device purchases by the Systems Division are made through Procurement in compliance with the Procurement Policy.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Administrative Services Division Management

## TARGET COMPLETION DATE

Completed.

## FINDING #3

| Finalize a complete mobile device inventory | Risk Rating[**] |
|---|---|
| | High |

## OBSERVATION

LACERA has over 270 mobile devices, approximately 180 of which are equipped with a cellular data line. The devices consist of 140 laptops, notebooks or netbooks, and 130 smartphones, tablets, and wireless hotspots. Administrative Services registers all laptops, notebooks, and netbooks in the Great Plains Fixed Asset Register. However, prior to October 2019, mobile phones and tablets were not recorded or tracked in Great Plains per prior Executive Office direction. Systems internally tracked those assets separately using Excel spreadsheets. As part of our testing, we requested all mobile device inventory listings from Systems

---

[**] See Appendix 2 for Finding's Risk Rating

which consisted of 1) wireless cellular lines, 2) smartphones and tablets registered to MaaS360, and 3) laptops registered to Microsoft Intune.

Per review of the wireless cellular lines and comparison to the MDM listings, we noted Systems had not completed a physical inventory, including spare, vacant, or test devices. Our review further identified areas to strengthen segregation of duties and controls around the mobile device inventory process. Specifically, mobile phones and tablets should be recorded and tracked in Great Plains, which represent an independent inventory list for validation against Systems internal records. Systems should also work in conjunction with Administrative Services to consistently perform an inventory of mobile devices including old, spare, obsolete and test devices.

## RISK

Without a complete and accurate list of active and inactive devices as well as an independent inventory register, LACERA may be susceptible to misappropriation or loss, lack of accountability for the deployment and use of devices, and increased costs.

## RECOMMENDATIONS:

3a. Systems Division management create a current mobile device master listing that includes all active, inactive, vacant, and test devices issued by LACERA. Systems to work with Administrative Services to record all mobile devices in Great Plains.

3b. Administrative Services and Systems management develop and implement a control-based mobile device inventory process. The process should include:
- Require execution of a formalized and documented annual inventory that includes active, inactive, vacant, and test devices.
- Documented responsibility for mobile device inventory asset accountability and tracking, device master listing maintenance, asset reconciliations and verification counts.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendations and plans to complete implementation by December 31, 2020. The Systems Division plans to continue maintaining the mobile device master listing outside of Great Plains to ensure appropriate recording of device information such as inactive, vacant, and test statuses. However, Systems will work with Administrative Services to ensure changes to the master listing are timely updated in Great Plains by Administrative Services.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Administrative Services Division Management

## TARGET COMPLETION DATE

December 31, 2020

## FINDING #4

| Register LACERA issued mobile devices to the mobile device management (MDM) tools | Risk Rating** |
|---|---|
| | Medium |

**AC Question: If MDM addresses encryption and thus security of data – why not a rating of High?**
**IA Response: We determined this was a Medium risk given LACERA adopted a standard of using and deploying Apple devices.  Apple devices have encryption features built in by default to safeguard data and Systems stated the 20 devices not registered were considered test devices.  In addition, none of the 21 Intune laptops are connected to the LACERA domain so do not represent a significant risk to LACERA's internal network.**

### OBSERVATION

As previously stated, LACERA has over 270 mobile devices of which 180 are equipped with a cellular data line. Our comparison of the wireless cellular lines to the MDM devices listings found that LACERA does not register all organization issued mobile devices to the respective MDM tools. Specifically, we noted approximately 20 mobile phones or tablets were not registered to MaaS360, and only 21 of 138 laptops were registered to Intune. Systems management stated it was a business decision and for technical logistics to not register all devices such as unassigned spare mobile phones or test devices used by Systems.  In some cases, it is also not technically possible to register not-yet deployed or configured devices in MDM. Systems further stated most of the other, typically older 117 laptops have hardware or software that are incompatible with Intune and expect future laptop purchases to meet those specifications.

**AC Question: What are the other mobile devices used for if they do not have cell access?**
**IA Response: Most of the mobile devices that do not have cell access are old or obsolete laptops that are not in use.**

### RISK

Mobile devices that have been deployed for production use but not registered to the MDM tools could be out of compliance with LACERA's MDM security policies and may be vulnerable to data leakage or unauthorized access.

### RECOMMENDATIONS:

4. Systems Division management define the organizational mobile device management (MDM) registration policy to be approved by the Executive Office. This should include documented exceptions to the policy, if any, approved by the Executive Office.

---

** See Appendix 2 for Finding's Risk Rating

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by October 31, 2020. Systems Division management will work with the Executive Office to define the appropriate organizational MDM registration policy for all devices including spare or test devices.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

October 31, 2020

## FINDING #5

| Define organizational baseline mobile device management (MDM) usage and security configurations | Risk Rating[**] |
|---|---|
| | Medium |

**AC Question: Why not High?**
**IA Response: We determined this was a Medium risk in recognition that LACERA does use MDM tools to centrally manage mobile devices.  In addition, Systems does have 6 different security configurations which highlight their focus on security considerations.**

## OBSERVATION

A mobile device baseline security configuration is a documented set of minimum specifications intended to prevent unauthorized use of mobile apps or device features vulnerable to cyber threats. Organizations commonly restrict users from performing certain functions on their assigned mobile devices to appropriately secure organizational devices and data. We observed that Systems does have six (6) different security configurations in the IBM MaaS360 tool; for example, a unique configuration for Board iPads, staff iPads, staff iPhones vs. test iPhones, etc. Generally, Systems Division management is also focused on security and while they may have created these configurations with specific intent, it was not defined and documented.

Further, we compared the settings against LACERA's *Unsafe Computer Practices Policy*, Federal standards as defined by the National Institute of Standards and Technology (NIST), and industry best practices. Our analysis determined that functions were not restricted within the various configurations to ensure compliance with LACERA's *Unsafe Computer Practices Policy*. For example, although the Policy prohibits users from installing mobile apps without Systems Division knowledge and consent, the Systems Division, per direction by the Executive Office preceding 2016, did not limit that functionality for end-users through the MDM tool.

---

[**] See Appendix 2 for Finding's Risk Rating

## RISK

LACERA may not be limiting its cyber security risks by ensuring device settings or features are appropriately restricted. This can leave a device exposed to vulnerabilities and weaknesses that cyber criminals could exploit.

## RECOMMENDATIONS:

5a. Systems management in conjunction with the Executive Office define organizational baseline mobile device management (MDM) usage and security configurations to strengthen device security. This should include limiting or restricting any high-risk functions with documented exceptions to the policy.

5b. Establish periodic review of policy settings to ensure they remain current with industry standards and best practices.

## MANAGEMENT'S ACTION PLAN

Management agrees with these recommendations and plans to complete implementation by October 31, 2020. The Systems Division evaluates security considerations in all implementation decisions and will work with the Executive Office to ensure appropriate operations objectives are met during this process.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

October 31, 2020

## FINDING #6

| Define a mobile device equipment standard that documents the business purpose by classification of recipients and a separate procedure for test devices | Risk Rating[**] |
| --- | --- |
| | High |

## OBSERVATION

In about 2012, LACERA adopted a standard of using and deploying Apple devices for mobile use. However, we noted that this was an informal decision by the Executive Office that was not documented.

Based on our analysis of System's wireless cellular list, we determined there were also sixteen (16) Android devices assigned to Systems staff and one Trustee in addition to their Apple devices. Systems management stated it was not the intention to include Android devices for mass deployment and those devices served testing and long-term evaluation purposes. However, we noted again that testing of these devices was informal without any documented purpose, plan or reporting of results, and was done without any formal Executive Office approval. In addition, we noted managers and staff are typically assigned between one and three mobile devices, those being a laptop, iPad and/or phone. However, we noted Systems Division

---

[**] See Appendix 2 for Finding's Risk Rating

management and or staff having up to 11 mobile devices each, including multiple phones and multiple tablets.

We verified six (6) individuals in the Systems Division were assigned more than one test device of the same type (e.g., two iPads) and often with the same wireless carrier and for an undetermined and extended period of time. Systems Division management stated it was common for staff to evaluate multiple test devices of the same brand but different models on the same wireless carrier to evaluate the different model's functionality with the carrier. However, we identified two instances where test devices of identical brand and model were used for testing on the same wireless carrier. In one instance by the same individual doing the testing. While testing of devices does not necessarily require wireless usage, we noted that these devices were all connected to wireless lines in calendar year 2019, but many of them had very minimal and virtually no or actually zero wireless usage in some cases.

Further, we noted Trustees typically receive an iPad and a laptop. We determined, however, one Trustee had 5 mobile devices including two tablets, one of them a Samsung android tablet test device, two laptops, and an active wireless hotspot still assigned to them but related to a previously returned laptop.

## RISK

Undocumented exceptions to organizational standards and policies regarding the deployment and use of mobile devices weakens the effectiveness of those standards and policies and could result in, at a minimum, the appearance of waste, fraud, and abuse.

## RECOMMENDATIONS:

6a. Systems Division Management should formalize and obtain Executive Office approval of mobile device issuance standards for staff and trustees and any exceptions to those standards should be documented and approved by the Executive Office.
6b. Systems Division Management should formalize and obtain Executive Office approval of a procedure for testing mobile devices.

**AC Question: Collect multiple devices currently assigned to individuals? (More than one of each device?)**
**IA Response: Systems Division Management and Executive Office should determine if this step is necessary as part of the remediation process.**

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendations and plans to complete implementation by October 31, 2020. The Systems Division will work with the Executive Office to define the mobile device issuance standards for staff, trustees, and test mobile devices.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

October 31, 2020

## FINDING #7

| Improve administration over mobile device acknowledgement and usage forms | Risk Rating[**] |
|---|---|
| | **High** |

## OBSERVATION

As previously stated, there are currently four (4) separate mobile device policies, which are incomplete and outdated. The staff policies include an area for signature/user acknowledgment, but we determined it was not obtained in practice. Alternatively, the Systems Division maintains a separate *Property Designation Form* for end users to sign when taking possession of the device.

Systems provided the signed Property Designations Forms for our audit testing as evidence that users acknowledge and abide by LACERA's mobile device policies. We noted that the form only contains acknowledgment of the quantity and type of devices issued and does not include acknowledgement that the user has read and will abide by LACERA's policies. Further, we determined that these acknowledgements are only obtained the first time a person receives a mobile device. No further acknowledgment was obtained either annually or when a similar device was replaced for the same user.

## RISK

Without current user acknowledgement forms, the organization may not be holding users accountable to their responsibilities, acceptable behavior, and usage restrictions of LACERA devices.

## RECOMMENDATIONS:

7. Systems Division management should improve the administrative process over mobile device acknowledgement and usage forms. The process should include the following:
   - Inclusion of the Form in the comprehensive and consolidated Mobile Device Management Policy.
   - Requirement that staff and Trustees re-sign a mobile device acknowledgement form annually and whenever provided a new device.

**AC Question: Is there a form signed by Systems when a device is returned, with a copy to the user?**
**IA Response:  Yes, Systems maintains a "Property Return Form" with a copy to the user.**

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by October 31, 2020.

---

[**] See Appendix 2 for Finding's Risk Rating

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management

## TARGET COMPLETION DATE

October 31, 2020

## FINDING #8

| Actively monitor and reconcile mobile device usage and wireless service costs | Risk Rating[**] |
|---|---|
| | High |

## OBSERVATION

As part of our testing, we analyzed all wireless bills for 2019 and noted the organization had an average of 189 wireless service lines, of which approximately 87 or 46% had limited or zero usage. Specifically, 15 wireless lines had usage fewer than 30 minutes and 72 had zero usage during 2019. Further, we noted 40 of the 87 limited or zero usage lines (46%) were designated as vacant or belonged to former staff or Trustees.

Systems staff verified that vacant lines are held to reserve the cellular number for LACERA's future use. Systems management also confirmed that some wireless lines were reassigned to current staff and some limited or zero usage devices serve a valid business purpose such as Disaster Recovery or Business Continuity. However, we noted only five reassigned lines in our testing of the 87 vacant lines reflected in the charts below, which summarize the devices usage and service costs for 2019. We also noted in December 2019, LACERA disconnected 61 of the vacant wireless lines as a result of the LA County Audit and those costs were eliminated.

**Zero Usage**

| Device Type | # of Devices | Annual Costs |
|---|---|---|
| Tablets | 28 | $ 8,812 |
| Laptops/Aircards | 32 | $ 7,623 |
| Cellphones | 7 | $ 3,661 |
| Smartphones | 5 | $ 1,884 |
| **Totals** | **72** | **$ 21,980** |

---

[**] See Appendix 2 for Finding's Risk Rating

**Limited Use***

| Device Type | # of Devices | Annual Costs |
|---|---|---|
| Smartphones | 5 | $ 3,018 |
| Tablets | 9 | $ 2,151 |
| Laptops/Aircards | 1 | $ 232 |
| **Totals** | **15** | **$ 5,401** |

* Less 30 minutes, 3 GB, or 36 Text Messages

In addition to limited or zero usage devices, we also reviewed the wireless bills for abnormal charges. Our review of the August 2019 billing cycle specifically identified abnormal international data roaming charges were incurred totaling $5,875. Appropriate documentation validating the costs and Executive Office approval for the additional charges was not retained.

**AC Question: Was approval for the additional charges obtained?**
**IA Response: The Verizon Plan in place at the time had a $1,000 limit on international data. Approval was provided to staff for the limit to be lifted for a traveler when they reported that their data had been cut off. The level of the approval for lifting the limit is unclear and was not documented. However, it was also not known at that time that the data usage would reach the cost that it did, over $4,000 for the one traveler in this instance. To be fair, this was not known to the traveler either. The important focus of this finding is having better oversight and management of wireless and data usage. Management has subsequently ensured that international travelers are placed in advance on unlimited international data plans at a very reasonable (approx. $10 per day) cost to LACERA. See answer to related question below.**

**AC Question: Are Trustees, or employees required to switch to an international plan for any overseas travel?**
**IA Response: The Board Secretaries, with the CEO's approval, will inform Systems when any Trustee travels overseas. Systems will setup the line/device to turn on the international package for the time the Trustee is abroad. Employees are case to case but generally follow a similar process.**

## RISK

Inadequate mobile device monitoring exposes the organization to additional costs, inefficient usage management, and could result in waste, fraud and abuse or the appearance of it.

## RECOMMENDATIONS:

8. Systems Division management establish guidelines approved by the Executive Office over the management and monitoring of wireless lines.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by September 30, 2020. The Systems Division has performed a reconciliation of wireless service lines in March 2020 to enhance documentation of some zero and limited usage lines as standby, backup, quick availability, and those maintained for legal holds. The finalization of further action items from the reconciliation has been delayed as the result of the COVID-19 pandemic; however, System's will complete those steps during implementation of this recommendation.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

September 30, 2020

## FINDING #9

| Strengthen mobile device deactivation, reassignment and disposal procedures | Risk Rating[**] |
|---|---|
| | High |

## OBSERVATION

To determine timely deactivation of wireless services and proper disposal of mobile devices, we examined the 2019 monthly wireless services bills for all carriers and inquired with staff regarding disposal procedures. We determined LACERA had approximately 40 wireless lines designated as "vacant" or belonged to former staff and Trustees. Although Systems management stated some devices were reassigned, we noted devices, some of which had belonged to staff or trustees who had left LACERA service up to five (5) ago, were still not reassigned. Further, we identified the following disposal procedures that required improvement:

- LACERA has not disposed of any old or obsolete tablets or smartphones since inception of the mobile device program.
- Formal documentation to validate that old or obsolete and devices returned by staff were appropriately reset to factory settings or the data was wiped is not maintained.
- A former Trustee's iPad is still considered outstanding according to the most recent Trustee inventory count performed by the Board Offices in December 2019.
- Former Trustees could purchase their LACERA issued iPad. However, documentation outlining the approval and process was not maintained.

---

[**] See Appendix 2 for Finding's Risk Rating

**AC Question: Was approval for the iPad purchases obtained?**

**IA Response: Per Systems Division Management, the prior CEO gave direction to Systems and announced at past Board Offsite meetings that Trustees could purchase their LACERA iPad.**

## RISK

Wireless services not disconnected timely could lead to unnecessary service charges. Inadequate reassignment and disposal of devices expose them to prolonged risks of misuse, theft or loss.

## RECOMMENDATIONS:

9.  Systems Division management develop a formal procedure approved by the Executive Office over the deactivation, reassignment, disposal and/or sale of mobile devices taken out of service. Additionally, this procedure should include the following:
    - A timeframe and methodology for the disposal of devices.
    - Formal documentation to validate that old, obsolete devices are appropriately reset to factory settings and wiped with a copy provided to the end user and Administrative Services.
    - An accurate inventory of out of service devices is maintained.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by October 31, 2020.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management
Executive Office

## TARGET COMPLETION DATE

October 31, 2020

## FINDING #10

| Strengthen administrative controls over restricting universal serial bus (USB) enabled workstations | Risk Rating[**] |
|---|---|
| | Medium |

## OBSERVATION

Per inquiry with Systems staff, Internal Audit noted the default LACERA workstation configuration enables USB access on all workstations. Systems then deploys a separate Group Policy Object (GPO), which is a collection of systems administrator settings that disables USB access to individual workstations. This process indicates that Systems must maintain a deny USB GPO list of 498 workstations. We noted a more effective approach would be to change the default setting to disable USB access during configuration and deploy a GPO that enables USB access. This will reduce the USB GPO listing to only approved workstations and assist Systems with performing a periodic review of approved workstations. Further, we

---

[**] See Appendix 2 for Finding's Risk Rating

found that there is no requirement or process to ensure that only encrypted USB devices are used for LACERA business.

## RISK

Inefficient controls over USB enabled workstations increases the risk of unauthorized transfer and removal of confidential LACERA information resulting in potential privacy incidents or breaches.

## RECOMMENDATIONS:

10. Systems Division management strengthen the process for managing workstations that have USB access enabled. The process should include:
    - A periodic review of USB enabled workstations to ensure such access is still appropriate.
    - A periodic reconciliation of the deny USB access listing against Administrative Services Fixed Asset Register.
    - Encryption required for USB devices connected to LACERA workstations.

## MANAGEMENT'S ACTION PLAN

Management agrees with the recommendation and plans to complete implementation by October 31, 2020.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Systems Division Management

## TARGET COMPLETION DATE

October 31, 2020

# APPENDIX 1
# AUDIT RATING SCALE

Internal Audit issues three standard audit report evaluations as defined below:

**Satisfactory**

The control environment is acceptable with minor issues having been identified. The overall environment contains sufficient internal controls to address key risks, and business practices generally comply with Company policies. Corrective action should be implemented to address any weaknesses identified during the audit in order to maintain or enhance the control environment.

**Opportunities for Improvement**

The control environment has opportunities for improvement with significant issues, individually or in the aggregate, having been identified or major noncompliance with Company policies. The overall environment contains insufficient internal controls to address key risks. Prompt corrective action should be implemented to address the weaknesses and strengthen the control environment.

**Unsatisfactory**

The control environment is unacceptable with critical issues, individually or in the aggregate, having been identified or major noncompliance with Company policies. The overall environment contains insufficient internal controls to address key risks and the impact may be substantial in size or nature or their effect cannot be quantified. Immediate corrective action should be implemented to address the weaknesses and strengthen the control environment.

## APPENDIX 2
## FINDING'S RISK RATING SCALE

Findings identified during the course of the audit are assigned a risk rating, as outlined in the table below. The risk rating is based on the financial, operational, compliance, or reputational impact that the issue identified could have on LACERA.

| Rating | Financial | Internal Controls | Compliance | Reputational | Executive Management |
|---|---|---|---|---|---|
| **High** | Large financial impact to LACERA or members<br><br>Actions not aligned with fiduciary responsibilities | Missing or inadequate key internal controls<br><br>Not adequate to identify fraud, noncompliance or misappropriation | Noncompliance with applicable Federal or state laws or LACERA's policies | High probability for external audit issues and/or negative public perception | Important critical business process identified by Exec Office<br><br>Requires immediate attention |
| **Medium** | Moderate financial risk to LACERA or members<br><br>Actions could be better aligned with fiduciary responsibilities | Partial key internal controls<br><br>Not adequate to identify noncompliance or misappropriation in timely manner | Inconsistent compliance with applicable Federal or state laws or LACERA's policies | Potential for external audit issues and/or negative public perception | Relatively important<br><br>May or may not require immediate attention |
| **Low** | Low financial impact to LACERA or members<br><br>Actions generally aligned with fiduciary responsibilities | Internal controls in place but not consistently efficient/effective<br><br>Implementing / enhancing controls could prevent future problems | General compliance with applicable Federal or state laws or LACERA's policies, but some minor discrepancies exist | Low probability for external audit issues and/or negative public perception | Lower significance<br><br>Does not require immediate attention |

# L CERA

June 16, 2020

TO:       2020 Audit Committee
          Gina V. Sanchez, Chair
          Keith Knox, Vice Chair
          Herman B. Santos, Secretary
          Vivian H. Gray
          David Green

          Audit Committee Consultant
          Rick Wentzel

FROM:     Richard Bendall
          Chief Audit Executive

          Kathryn Ton
          Senior Internal Auditor

FOR:      June 25, 2020 Audit Committee Meeting

SUBJECT:  **Contract Management System (CMS) Audit**

## RECOMMENDATION

**In accordance with the current Audit Committee Charter, staff recommends that the Audit Committee review and discuss the following engagement report to take the following action(s):**

1. **accept and file report and/or,**
2. **instruct staff to forward report to Boards or Committees and/or,**
3. **provide further instruction to staff.**

## ENGAGEMENT REPORTS

a. Contract Management System (CMS) Audit
   Kathryn Ton, Senior Internal Auditor
   (Report issued: June 15, 2020)

Attachments

KT

**LACERA INTERNAL AUDIT DIVISION**

**CONTRACT MANAGEMENT SYSTEM (CMS) AUDIT**

June 15, 2020

**AUDIT PERFORMED BY:**
Kathryn Ton, CPA, CFE
*Senior Internal Auditor*

# AUDIT REPORT

| Audit Name: | Contract Management Audit |
|---|---|
| Responsible Division: | Administrative Services |
| Audit Rating*: | Opportunities for Improvement |
| Prior Audit Rating*: | Not Applicable |
| Prior Report Date: | June 19, 2018 |

## BACKGROUND

We reviewed LACERA's contract management program as part of the Fiscal Year 2019-2020 audit plan. An effective contract management program is important because it mitigates potential risks associated with noncompliance. LACERA's contracting process is decentralized. Each division is responsible for the administration and management of its contracts, with some oversight by the Administrative Services Division (Admin Services).

The Contract Management System (CMS) developed as an in-house application by LACERA's Systems Division, intended to provide Admin Services the ability to:

1. Maintain a central repository of LACERA contracts.
2. Record key data fields from the contracts to be used in generating reports to both assist the decentralized contract managers with contract due diligence and compliance, as well as to provide Admin Services with some oversight of the decentralized contract management to validate compliance.
3. Send automatic notifications to contract managers about contract expirations and due diligence requirements.
4. Provide contract managers access to view their contracts in the application.

The scope of this audit was limited to assessing the effectiveness of the CMS application in these intended roles and in facilitating contract compliance. Our audit scope was limited to interviews of Admin Services management and staff, and interviews and surveys of contract managers. We did not perform contract management compliance testing of any contracts. We will perform compliance testing of a sample of LACERA contracts in the Fiscal Year 2020-2021 Audit Plan.

In calendar year 2019, 27 LACERA contract managers initiated 66 new contracts, or 20% of the total 320 contracts in the CMS. The CMS tracks all LACERA contracts, except for investment-related service contracts. For investment-related services, purchases are delegated to the Chief Investment Officer in accordance with the Procurement Policy for Investment-Related Services. LACERA enters into various contracts related to the purchase of goods and services. A contract

---

* See Appendix 1 for Audit Rating

manager is involved in every aspects of the contract, from pre-contracting due diligence and contract acquisition to contract management and contract closeout.

The Legal Office, Admin Services, and Financial Accounting Services Divisions (FASD) support contract managers throughout the contracting process. The Legal Office mitigates risk by drafting and reviewing contracts to obtain the best terms and conditions for LACERA. The Procurement Policy requires the Legal Office to review all engagements above $5,000, or engagements that may elevate risk to member data, LACERA's personnel, facilities, or systems.

Admin Services ensures that each contract complies with the Procurement Policy and contractual terms and conditions. In addition, Admin Services oversees the CMS and provides contract managers with reminders and prompts regarding contract actions. In the payment process, Admin Services' Budget Team first reviews all payment requests for determination of the appropriate budget codes being applied, and then the Contract Unit reviews all payment requests to validate that there is an active contract and that all payment terms are in alignment with the contract. FASD then reviews invoices and processes them for payment.

The Systems Division and Internal Audit are also engaged by contract managers in both the pre-contract due diligence stage and ongoing due diligence of contracts where LACERA member data will be provided to and or accessed by vendor(s). This includes reviews of the vendors' IT security practices or Service Organization Control (SOC 2) reports from the vendors' external auditors, if any. The Systems Division and Internal Audit will sometimes perform a site visit to the vendors' facilities to ensure that appropriate physical and virtual controls exist to protect LACERA information. This was not part of the scope of this review but will be tested in the follow-up compliance audit next fiscal year.

Effective contract oversight requires that effective controls exist throughout the contracting and payment processes.

## AUDIT OBJECTIVE AND SCOPE

The audit objectives were to determine the effectiveness of the CMS in facilitating contract compliance. The diagram below illustrates the responsible parties involved when administering a contract management program.
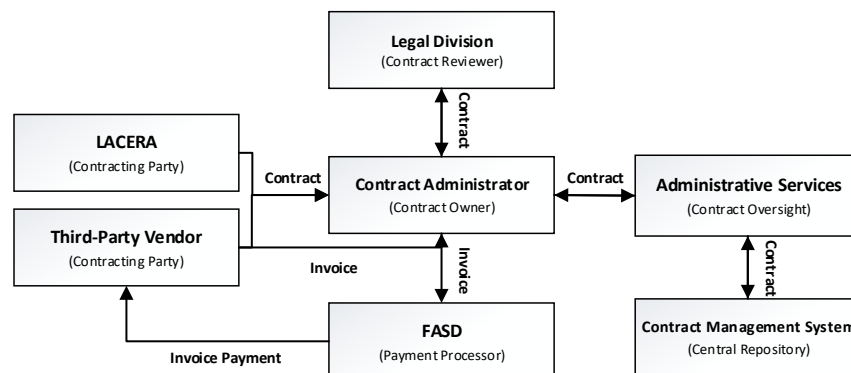
The audit scope covers calendar year 2019 and involved:

- Discussions with Admin Services staff about administering the CMS.
- Review of LACERA's CMS training procedures.
- Review of LACERA's 2006 and 2019 Procurement Policies.
- List of contract managers and contracts as of December 2019.
- Review of contracts in CMS and user access controls.
- Contract manager questionnaire and data analytics on responses.
- Review of LACERA's contract compliance procedures.
- Controls testing to determine whether operations are performed according to established procedures.

*Note: Internal Audit did not review employment contracts (Human Resources) or investment manager contracts (Investments Office), because these contracts are not maintained in the CMS.*

The audit was performed in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

## AUDIT RATING AND SUMMARY OF FINDINGS

Overall, Internal Audit found the CMS to be operating as intended and providing Admin Services the ability to maintain a repository of LACERA contracts and the ability to have oversight over compliance and due diligence over those contracts. However, we did note some areas where **Opportunities for Improvement** could be made to strengthen the CMS as a control in the contract management process. We also determined through our survey of contract managers the desire for a more comprehensive CMS application that provides contract managers with additional functionality and access.

Summary of Findings

| Ref. | Page | Finding | Risk Rating** |
|------|------|---------|---------------|
| F1 | 6 | Strengthen controls in the administration of the current CMS application. | Medium |
| F2 | 8 | Evaluate the need to enhance the CMS application to provide improved functionality. | Low |

Each of the above findings are detailed in the following pages, including our recommendations and management action plans.

We would like to thank the contract managers and Administrative Services Division for their cooperation with this audit.

---

** See Appendix 2 for Finding's Risk Rating

**REVIEWED AND APPROVED**

_____     **Date:**   June 15, 2020

Richard Bendall
*Chief Audit Executive*

**REPORT DISTRIBUTION**

| | | |
|---|---|---|
| 2020 Audit Committee | Santos H. Kreimann, CEO | Kimberly Hines, Administrative Services Division Manager |
| 2020 Plante Moran Audit Team | J.J. Popowich, AEO | Internal Audit Group |
| Rick Wentzel, Audit Committee Consultant | Steven Rice, Chief Legal Counsel | |

## FINDING #1

| Strengthen controls in the administration of the current CMS application | Risk Rating** |
|---|---|
| | Medium |

### OBSERVATION

While the current CMS application was not intended to be a completely holistic contract management system, we did note, based on our interviews and surveys, opportunities to improve controls surrounding and usability of the current system: Specifically:

1a. CMS Data Accuracy – Contract managers complete transmittal forms related to each contract with the key contract data information, and provide these to Admin Services who enter the data in the CMS. In February 2019, in an effort to review and clean the legacy data that resides in the CMS system, Admin Services provided division managers and contract managers a list of their CMS contracts and metadata.  Some responded to the request, but most of them did not. Admin Services should hold contract managers accountable and perform more frequent reviews to ensure that all data in the CMS is up to date, complete, and accurate.

1b. CMS Functionality – Through the CMS, Admin Services sends email reminders to the decentralized contract managers in all LACERA's divisions. This provides Admin Services the ability to ensure compliance in the contract management process across divisions, and provides contract managers with assistance in staying on top of contract management. While the CMS was built with the ability to send email reminders directly to contract managers, Admin Services management informed us they have not yet turned this feature on, primarily due to the need for completing the training manual and providing contract managers with further training, discussed below. Currently, the CMS sends all automatic reminders to Admin Services, who then has to perform additional analysis to ensure that the information is accurate and complete, before manually emailing the reminders to the contract managers.

1c. Training of Contract Managers – It is a best practice to develop and implement a contract administration manual that aligns with current policies and practices. At the time of this audit, the Purchasing & Contract Administration Manual had not been updated to reference the Procurement Policy adopted in November 2019 as well as any updates made to the CMS application. Necessary revisions include updating contracting terms, contract schedules, contract signing authority, and other information related to contract administration and due diligence. On February 28, 2020, the Purchasing & Contract Administration Manual was completed and communicated to staff; however, formal training has not been conducted to educate contract administrators and managers.

---

** See Appendix 2 for Finding's Risk Rating

Our survey identified that contract managers lacked a complete understanding of either their contract management responsibilities or an understanding of the functionality, usability, and responsibilities relating to the CMS application. Survey results indicated further that although contract managers can readily access their contracts on the CMS, less than half of them ever do (44%). This is the result of the contract managers' unfamiliarity with the product. We found that even though Admin Services provided contract managers with initial CMS training (February 2019), new contract managers assigned after that date received no formal training.

## RISK

Without employing the full functionality of a system, ensuring the accuracy of the data in the system and training users on the functionality of the system as well as their responsibility over it, the risk of the system not being used or failing in its intended use is significantly increased.

## RECOMMENDATIONS:

Administrative Services should:

1a. Ensure that contract managers perform periodic reviews, at least quarterly, of data in the CMS for which they are responsible and confirm the accuracy of the data.

1b. Complete the intended implementation of the current CMS system's functionality by activating the direct email function of reminders/prompts from the CMS to contract managers.

1c. Provide comprehensive training to all division managers and their delegated contract managers.

## MANAGEMENT'S ACTION PLAN

Administrative Services will:

1a. Implement a quarterly review process with contract managers to confirm that the data in the CMS is accurate.

1b. Implement/activate the CMS functionality related to automatically sending email reminders/prompts to contract managers.

1c. Provide comprehensive training to all division managers and their delegated contract managers.

## RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Administrative Services

## TARGET COMPLETION DATE

1a. December 31, 2020

1b. December 31, 2020

1c. December 31, 2020

## FINDING #2

| Evaluate the need to enhance the CMS application to provide improved functionality | Risk Rating[**] |
|---|---|
| | Low |

### OBSERVATION

Our survey of contract managers also identified a desire to enhance the current CMS application. Beyond the additional functionality that is planned for the existing system, a number of contract managers expressed interest in a more comprehensive system which includes features such as automated workflows to facilitate contract development and approvals, facilitation of contract compliance monitoring, and a system which connects contracts to LACERA's budgeting and payment systems for tracking and monitoring of contracts.

### RISK

Efficiencies, effectiveness, and consistencies of contract development and management could be greatly enhanced through a more comprehensive contract management application.

### RECOMMENDATIONS:

2. Administrative Services should evaluate the needs of the contract managers and the organization, and provide a written report to the Executive Office with recommendations to enhance the current CMS application or a recommendation to seek another product that will meet LACERA's needs.

### MANAGEMENT'S ACTION PLAN

Administrative Services will evaluate the needs of the contract managers and the organization. A written report with recommendations will be provided to the Executive Office with recommendations to either enhance the current CMS application or to seek another product that will meet LACERA's needs.

### RESPONSIBLE PARTY FOR MANAGEMENT'S ACTION PLAN

Administrative Services

### TARGET COMPLETION DATE

November 30, 2020

---

[**] See Appendix 2 for Finding's Risk Rating

# APPENDIX 1
# AUDIT RATING SCALE

Internal Audit issues three standard audit report evaluations as defined below:

**Satisfactory**
The control environment is acceptable with minor issues having been identified. The overall environment contains sufficient internal controls to address key risks, and business practices generally comply with Company policies. Corrective action should be implemented to address any weaknesses identified during the audit in order to maintain or enhance the control environment.

**Opportunities for Improvement**
The control environment has opportunities for improvement with significant issues, individually or in the aggregate, having been identified or major noncompliance with Company policies. The overall environment contains insufficient internal controls to address key risks. Prompt corrective action should be implemented to address the weaknesses and strengthen the control environment.

**Unsatisfactory**
The control environment is unacceptable with critical issues, individually or in the aggregate, having been identified or major noncompliance with Company policies. The overall environment contains insufficient internal controls to address key risks and the impact may be substantial in size or nature or their effect cannot be quantified. Immediate corrective action should be implemented to address the weaknesses and strengthen the control environment.

# APPENDIX 2
## FINDING'S RISK RATING SCALE

Findings identified during the course of the audit are assigned a risk rating, as outlined in the table below. The risk rating is based on the financial, operational, compliance, or reputational impact that the issue identified could have on LACERA.

| Rating | Financial | Internal Controls | Compliance | Reputational | Executive Management |
|---|---|---|---|---|---|
| **High** | Large financial impact to LACERA or members<br><br>Actions not aligned with fiduciary responsibilities | Missing or inadequate key internal controls<br><br>Not adequate to identify fraud, noncompliance or misappropriation | Noncompliance with applicable Federal or state laws or LACERA's policies | High probability for external audit issues and/or negative public perception | Important critical business process identified by Exec Office<br><br>Requires immediate attention |
| **Medium** | Moderate financial risk to LACERA or members<br><br>Actions could be better aligned with fiduciary responsibilities | Partial key internal controls<br><br>Not adequate to identify noncompliance or misappropriation in timely manner | Inconsistent compliance with applicable Federal or state laws or LACERA's policies | Potential for external audit issues and/or negative public perception | Relatively important<br><br>May or may not require immediate attention |
| **Low** | Low financial impact to LACERA or members | Internal controls in place but not consistently efficient/effective<br><br>Implementing / enhancing controls could prevent future problems | General compliance with applicable Federal or state laws or LACERA's policies, but some minor discrepancies exist | Low probability for external audit issues and/or negative public perception | Lower significance<br><br>Does not require immediate attention |

# LACERA

June 16, 2020

TO:        2020 Audit Committee
                Gina V. Sanchez, Chair
                Keith Knox, Vice Chair
                Herman B. Santos, Secretary
                Vivian H. Gray
                David Green

                Audit Committee Consultant
                Rick Wentzel

FROM:    Richard Bendall
                Chief Audit Executive

                Summy Voong
                Senior Internal Auditor

FOR:     June 25, 2020 Audit Committee Meeting

SUBJECT:   **Clear Skies Penetration Test and Veracode Static Code Analysis**

**PENETRATION TEST**

As part of the Fiscal Year 2019 – 2020 Audit Plan, Internal Audit (IA) hired Clear Skies Security LLC (Clear Skies) to perform a penetration test of LACERA's network, systems, and applications that comprise of the organization's internet presence. The objective of the assessment was to evaluate the information security of the network from an external perspective to determine any risks posed from an uncredentialed attacker. The penetration test was designed to identify security issues in LACERA's environment and to put those risks in the context of both the IT and business environments. Internal Audit periodically performs these types of security assessments as a best practice and last completed a similar review that was reported at the July 2019 Audit Committee meeting. This memorandum and the attached Executive Summary provide the results of Clear Skies' assessment.

Based on the results of the penetration test, Clear Skies considers the tested LACERA systems to be at an overall Medium level of risk. This represents a moderately elevated exposure level from an external perspective compared to other organizations assessed by Clear Skies. A total of one high, eight medium, and twenty-nine low risks vulnerabilities were noted; however, none of these ultimately led to direct unauthorized access to systems or data in LACERA's systems. Clear Skies recommends addressing the high and medium risk issues in the short term and addressing low risks items when possible.

## VERACODE STATIC CODE ANALYSIS

In addition to the penetration test, Clear Skies also performed a static code analysis of the MyLACERA application using Veracode's application security service to identify potential security vulnerabilities in the application code. Veracode is an application security company that provides automated cloud-based services for securing web, mobile, and third-party enterprise applications. Clear Skies reviewed the application to the extent possible to validate the issues flagged as vulnerabilities by the Veracode service and noted that many are likely to be false positives with no security risk. One medium and two medium/low risks vulnerabilities did appear to be valid but are of limited exploitability. A summary and full report of the Veracode results with Clear Skies' comments have been provided to management as part of this assessment.

## MANAGEMENT ACTION PLANS

Systems Division Management agrees with all issues noted and has action plans in place or under evaluation to mitigate all risks identified in this assessment. Internal Audit also plans to have Clear Skies perform re-testing once many of the issues have been remediated. Staff will continue to provide updates to the Committee regarding future results of the security assessment.

We would like to thank the Systems Divisions for their cooperation with this security assessment.

## REVIEWED AND APPROVED

_____          **Date:** June 16, 2020

Richard Bendall
*Chief Audit Executive*

## MEMORANDUM DISTRIBUTION

| 2020 Audit Committee | Santos H. Kreimann, CEO | James P. Brekk, Systems Division Manager |
|---|---|---|
| Rick Wentzel, Audit Committee | J.J. Popowich, AEO | Internal Audit Group |
| | Steven Rice, Chief Legal Counsel | |

# Clear Skies

## SECURITY

### Intelligence. Secured.

# Penetration Test
# Executive Summary

Los Angeles County Employees
Retirement Association
(LACERA)

June 2020

# Executive Summary

Los Angeles County Employees Retirement Association ("LACERA") engaged Clear Skies Security LLC ("Clear Skies") to undertake a comprehensive security assessment known as a Penetration Test of the network, systems, and applications that comprise the LACERA internet presence. Initial testing occurred from Feb 3-Mar 4, 2020. Retesting of any identified vulnerabilities will be conducted upon LACERA's request once all issues have been remediated

The objective was to assess the information security posture of the network from an external perspective to determine risks posed from an uncredentialled attacker.

The Clear Skies Penetration Test is designed to identify security issues in the target environment, and more importantly, to put them in the context of the IT and business environment.

All identified security controls and weaknesses are evaluated as a whole to clearly demonstrate the potential impact on the environment so that the organization may target tactical and strategic initiatives where the need is most acute. By subjecting the environment to testing, LACERA has demonstrated a strong commitment to understanding their true security posture and developing concrete risk mitigation strategies.

## RISK PROFILE

Based on the results of this test, Clear Skies considers the tested LACERA systems to be at a **Medium** level of overall risk. Compared to other organizations assessed by Clear Skies, the LACERA environment tested in this engagement has an moderately elevated exposure level from an external perspective.

From a general network perspective, the LACERA environment exposes a relatively small attack surface. Other than the MyLACERA application and public web site, only a handful of firewall, remote access, and administrative services are present.

### Risk Summary

M    Medium Risk

### Threat Levels

L    System Compromise
H    Information Loss
L    Service Disruption

### Risk Chart

Easy Exploitation
No Critical Data

Difficult Exploitation
No Critical Data

Exploitation Difficulty

Data Exposure

Easy Exploitation
Very Critical Data

Difficult Exploitation
Very Critical Data
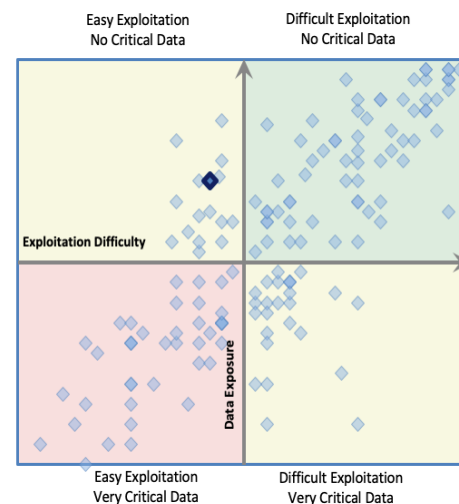
## VULNERABILITIES & RECOMMENDATIONS

A total of one high risk, eight medium risk, and twenty-nine low risk vulnerabilities were noted. None of these ultimately resulted in direct unauthorized access to systems or data in the target systems. Some of the issues identified could nevertheless have an adverse impact in some scenarios.

All vulnerabilities identified can typically be remediated with relatively low effort. Clear Skies recommends addressing the high and medium risk issues in the short term and addressing low risk items as possible.

From a network perspective, only medium and low risk issues were identified in systems outside the MyLACERA application. Notably, all medium risk vulnerabilities are in the public web site search component, which were also noted in testing from 2014. Upgrading or replacing the outdated components and applying best practice configurations to the web services would address many of the issues noted.

The overall elevated exposure level is due primarily to the behavior of an application when handling network communication requests. Several other weaknesses as detailed in the full report can also result in unauthorized access to a user's account under more limited circumstances. A significant number of other low risk issues were found, primarily related to authentication, session management, and configuration.

### Total Vulnerabilities

1    8

29

■ High  ■ Medium  ■ Low

### Affected Systems

100%

60%

50%                30%

10%

0%

■ High  ■ Medium  ■ Low

The application does offer controls that provide a good security foundation. For example, logins from new devices are not allowed until a user answers their secondary security questions. Lockouts after failures limit brute force attacks, although there were instances in which this control could be bypassed. Request tokens effectively prevent Cross-Site Request Forgery attacks in which an outside attacker constructs requests that are triggered in the application when followed by authorized users. No issues at all were identified related to internal access controls or insecure handling of user input.

Lastly, other than automated request lockouts, there was no indication during testing that any of the reconnaissance, vulnerability scanning, or other testing was detected or blocked. LACERA should review these results in relation to the detection capabilities to ensure they are working as intended and are improved where appropriate.
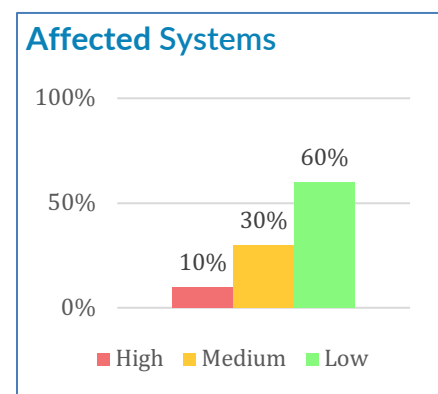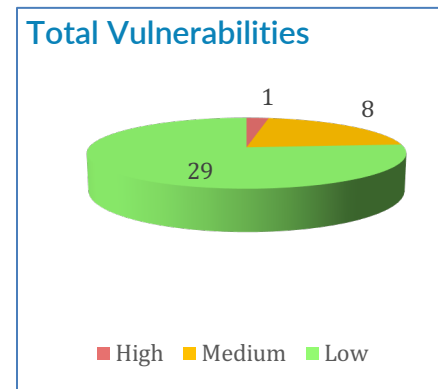
# About Clear Skies Security

According to recent research "massive data fraud and theft" and "cyber-attacks" are now ranked in the top five enterprise risks by likelihood over the next ten-year period. Compounding this is the fact that machine learning and artificial intelligence are becoming more sophisticated and will ultimately be used to assist hackers in amplifying these risks. This trend is at the very core of why Clear Skies Security was founded – the rules of the game are changing, and organizations cannot continue to rely on the same kinds of testing that has been done in the past.

Although most organizations understand the need to protect critical enterprise environments, the reality is that many remain at risk mostly due to the lack of specialized security expertise. The main advantage Clear Skies offers our customers is our people - true industry leaders in the assessment arena.

We start by understanding our customer's business objectives because we know that security is not a one-size-fits-all process. The goal of each assessment is to view it as a unique environment. Although a standard methodology is followed for all of our assessments, each engagement is thoroughly reviewed by a senior consultant that understands the cascading effects vulnerabilities can have. The results of every project are then manually reviewed and verified – relying on the experience of the tester and not an automated scanner. This is a critical differentiator in today's world of emerging threats. The end result is a comprehensive approach to a risk management solution, which can be understood by both technical and executive staff.

Clear Skies Security was founded by a team of elite security professionals, each bringing 20+ years of experience in the security industry, all with a specialty in security assessments. Our mission is to be a trusted name in the security industry, known for our technical knowledge, integrity, and business ethics. We do this by focusing on customer service and ensuring quality in everything we do.

In the end, our goal is to ensure that our Intelligence Secures your Intelligence.

# L CERA

June 16, 2020

TO:     2020 Audit Committee
          Gina V. Sanchez, Chair
          Keith Knox, Vice Chair
          Herman B. Santos, Secretary
          Vivian H. Gray
          David Green

          Audit Committee Consultant
          Rick Wentzel

FROM:   Richard Bendall
          Chief Audit Executive

          Nathan Amick
          Internal Auditor

FOR:    June 25, 2020 Audit Committee Meeting

SUBJECT:  **Audit of Foreign Payees**

## RECOMMENDATION

**In accordance with your current Audit Committee Charter, staff recommends that the Audit Committee review and discuss the following engagement report to take the following action(s):**

1. **accept and file report and/or,**
2. **instruct staff to forward report to Boards or Committees and/or,**
3. **provide further instruction to staff.**

## ENGAGEMENT REPORTS

a. Audit if Foreign Payees
   Nathan Amick, Internal Auditor
   (Report issued: April 29, 2020)

Attachments

NKA

**LACERA INTERNAL AUDIT DIVISION**

## Audit of Foreign Payees

April 29, 2020

**AUDIT PERFORMED BY:**
Nathan Amick, CIA
*Internal Auditor*

## EXECUTIVE SUMMARY

Internal Audit completed an audit of foreign payees to verify the "alive and well" status of all retirement payees with a foreign address on file, including those addresses in U.S territories, i.e. Puerto Rico, Guam, American Samoa.

Timely identification of deceased members is imperative to prevent overpayments and deter fraud. Member deaths are reported to LACERA by various parties including family, friends, past County department employers, funeral homes, coroners, hospitals, etc. However, these channels are not always effective in reporting deaths timely. Therefore, LACERA created the member death verification process, performed by the Benefits Division's Benefit Protection Unit (BPU), to supplement the regular notification channels to ensure that deaths are identified as timely as possible.

The member death verification process consists primarily of BPU staff working with the "death verification contractor" (DVC), which is a company that provides death match services to pension funds and other financial services firms. The DVC compiles death data from various sources including the Social Security Administration (SSA), Railroad Retirement Board, Department of Veterans Affairs, Civil Service Commission, and obituary information. The DVC also purchases vital statistics data that include state death records, marriage records, and birth records from public health agencies and vital statistics offices across the country. Not all states make vital records public and available for purchase.

Deaths of members residing outside of the United States are far less likely to be reported to these agencies and may not be identified via the member death verification process. Consequently, LACERA must verify the status of the foreign payees by performing periodic audits of their living status.

The audit objective was to confirm the "alive and well" status of all 227 (100%) foreign payees on record as of Jan 14, 2019. For this audit we defined foreign payees as those retirement payees whose address on record is outside of the 50 United States.

The means to determine the foreign payees "alive a well" status was a threefold mailing process requiring the member to either call LACERA to be verified, or submit the required documents verified by a U.S. Consulate or U.S. Embassy. For those foreign payees who were not verified as a result of the mailing process their case was referred by BPU to a third-party investigative service, Covent Bridge Group (CBG) to provide assistance in the verification process.

Based on our audit test work of the 227 foreign payees, 206 responded to the "Payee Status Verification Letter" and were verified as alive by LACERA. Seven (7) more were determined deceased by LACERA's normal death verification process during the period of our audit. The remaining 14 were referred to CBG for wellness visits including one that LACERA suspected may be deceased. CBG was able to visit and validate twelve (12) were "alive and well," one (1) was deceased, and the other one (1) suspected deceased could not be validated as either alive or dead by either LACERA or CBG and the members retirement will remain on hold.

# Audit of Foreign Payees

## INTRODUCTION

Internal Audit completed an audit of foreign payees to verify the "alive and well" status of all retirement payees with a foreign address on file, including those addresses in U.S territories, i.e. Puerto Rico, Guam, American Samoa.

The last foreign payee audit was completed in October of 2015. As a result of this audit, Internal Audit verified 203 of all 209 foreign payees, including 4 deceased, at that time. The remaining six of the 209 foreign payees could not be contacted and/or verified, so their accounts were put on hold. Prior to the initiation of this audit, three of the six unverified have since been verified as alive and have had their accounts reinstated. The remaining three have been verified as deceased.

## BACKGROUND

Timely identification of deceased members is imperative to prevent overpayments and deter fraud. Member deaths are reported to LACERA by various parties including family, friends, past County department employers, funeral homes, coroners, hospitals, etc. However, these channels are not always effective in reporting deaths timely. Therefore, LACERA created the member death verification process, performed by the Benefits Division's Benefit Protection Unit (BPU), to supplement the regular notification channels to ensure that deaths are identified as timely as possible.

The member death verification process consists primarily of BPU staff working with the "death verification contractor" (DVC), which is a company that provides death match services to pension funds and other financial services firms. The DVC compiles death data from various sources including the Social Security Administration (SSA), Railroad Retirement Board, Department of Veterans Affairs, Civil Service Commission, and obituary information. The DVC also purchases vital statistics data that include state death records, marriage records, and birth records from public health agencies and vital statistics offices across the country. Not all states make vital records public and available for purchase.

Deaths of members residing outside of the United States are far less likely to be reported to these agencies and may not be identified via the member death verification process. Consequently, LACERA must verify the status of the foreign payees by performing periodic audits of their living status

## AUDIT OBJECTIVES

Confirm the "alive and well" status of all foreign payees. For this audit we have defined foreign payees as those retirement payees whose address on record is outside of the 50 United States, including those with addresses in U.S territories, i.e. Puerto Rico, Guam and American Samoa.

## AUDIT SCOPE

Review LACERA's Foreign Payee Data File – Internal Audit requested and obtained from the Systems Division a foreign payee data file. The file contained 227 (100%) individuals with foreign addresses on record as of Jan 14, 2019.

Included in this population of 227 were three payees LACERA placed on hold as a result of the 2015 Foreign Payees Audit as they could not be validated "alive and well" during that audit. They subsequently validated their living status and LACERA reinstated their retirement payments.

## AUDIT METHODOLOGY

Starting in February 2019, the BPU mailed each foreign payee a "Payee Status Verification Letter." The letter explained the verification options available to the member, which included:

1) Calling into LACERA and correctly answering the High Risk Identification questions, or;

2) Having the appropriate government agency (U.S. Consulate or U.S. Embassy) complete LACERA's "Request for Confirmation of Identity Form" after reviewing the member's identification document(s). Members are then required to mail the form to LACERA.

BPU sent a second verification letter, 30 days after the initial verification letter, was sent to those payees who did not successfully complete the required verification. This second letter provided the same verification request. 60 days after the initial verification letter, a third and final letter was sent to inform the member that their benefits will be placed on hold beginning June 1, 2019 if not properly verified.

For those foreign payees that failed the High Risk ID verification questions by telephone or did not have the means to travel to the required government agency to be verified, the case was referred by BPU to a third party investigative service, Covent Bridge Group (CBG), to provide assistance in the verification process. Additionally, if we had received no contact from the member after the third letter, the case was also referred to CBG to provide assistance in the verification process.

Covent Bridge Group is one of the insurance industry's premier full-service evidence provider specializing surveillance, claims investigation, and counter-fraud programs. LACERA uses CBG both locally and abroad to assist in the member verification process. At BPU's request, CBG conducts in-person "Alive and Well Checks." For LACERA's purposes, an Alive and Well Check consist of all of the following:

- Face-to-face visit with the member
- Review documentation of the member's identification (driver's license, passport, etc.)

- Conducting a high-risk questionnaire. This questionnaire is created by Internal Audit and is similar in form to the authentication Member Services performs when the members call in to be verified.
- Having the member sign a LACERA-created "Sworn Statement" attesting to their identity and that they are a valid LACERA member eligible for a monthly benefit.

## AUDIT RESULTS

Based on our audit test work of the 227 foreign payees, 206 responded to the "Payee Status Verification Letter" and were verified as alive by LACERA. Seven (7) more were determined deceased by LACERA's normal death verification process during the period of our audit. The remaining 14 were referred to CBG for wellness visits including one that LACERA suspected may be deceased. CBG was able to visit and validate twelve (12) were "alive and well," one (1) was deceased, and the other one (1) suspected deceased could not be validated as either alive or dead by either LACERA or CBG and the members retirement will remain on hold.

**Verified Alive**
- 206 (91%) of the 227 foreign payees were verified alive as indicated below:
  - o 183 of the 206 – member called LACERA's Call Center and successfully passed the high risk ID verification process as performed by Call Center Staff.
  - o 23 of the 206 – member responded via mail by submitting the "*Request for Confirmation of Identity Form*" completed by a US Embassy or Consulate within the foreign country of residence of the payee. BPU staff was responsible for reviewing the documents and determining the member's alive status.

**CBG Investigation Referrals**
- 14 (6%) of the 227 foreign payees were referred by BPU to CBG for an in-person "alive and well" check:
  - o 12 of the 14 - CBG investigators met with members in-person and verified them as alive.
  - o One of the 14 - CBG investigator verified the member deceased, July 25, 2018.
    - ▪ LACERA received no response from its three "Payee Status Verification Letter" mailings, and the case was referred to CBG for an in-person "alive and well" check. CBG was unable to initiate any contact with the member and decided to perform an impromptu visit to the address of record. CBG was unable to make contact during their visit, however they did talk to neighbors who stated that the member had died approximately two years ago.

- Based on the information provided by neighbors, CBG was able to track down a copy of the member's death certificate. Per the death certificate the member died July 25, 2018.
- Based on the July 25, 2018 date of death and the June 20, 2019 payment hold placed on the member's account, LACERA made a total overpayment to the decedent in the approximate amount of $5,440 (10 mos. X $544).
- BPU has requested a certified original copy of the decedent's death certificate. Once BPU receives the death certificate the case will be forwarded to the Benefit's Account Settlements Unit who will attempt to recoup the overpayment.

- One of the 14 - CBG exhausted all efforts and resources in their attempts to make contact. A pay hold was placed on the member's account as of June 20, 2019, and the member was placed on the "Persons of Interest" report.

## Verified Deceased
- Seven (3%) of the 227 foreign payees were determined to be deceased and their payments were stopped.
  - Three of the seven – verified as deceased with the member's death and the death notification to LACERA occurring during our testing time frame.
    - In all three cases a relative/friend called LACERA's Call Center to report the member's death, and later an original death certificate was received and verified by the Benefits Division's Death Legal Unit.
    - While our testing may have prompted these death notifications, we cannot confirm this assumption.

  - Three of the seven – verified as deceased by LACERA's BPU as a result of their normal death verification procedures. These death verifications were not a result of our testing procedures.
    - In all three cases the death verification was identified, confirmed, and reported to the BPU by LACERA's "death verification contactor."
    - One case resulted in LACERA recouping three months of overpayments in the approximate amount of $2,652 ($869 X 3 mos.).
    - While the death identification, and the recoupment of the $2,652 in overpayments was not a result of Internal Audit's testing, our testing procedures did aide in limiting the overpayments. Had it not been for Internal Audit's testing and the resulting payment hold of June 20, 2019,

the overpayments would have continued another two months in the amount of $1,738 ($869 X 2 mos.).

- o One of the seven – reported as deceased but the death could not be verified. LACERA was notified of the member's death via phone call in January 2016. The caller had no specific info other than the member was deceased.
  - BPU immediately began looking into the case and identified ten uncashed checks dating back to May of 2015 in the approximate amount of $12,670 ($1,267 X 10 mos.). In March of 2016 BPU placed a payment hold on the member's account, and stop payments were executed on all ten uncashed checks.
  - As of August 25, 2016, the BPU had exhausted all efforts to certify death with a valid death certificate and date of date. At this time BPU had the account locked and the payment hold remained in place.
  - With there being no death certificate and no date of death, the decedents account cannot be inactivated, thus the account remains active with a hold and lock in place. As long as the account remains active the decedent will remain in the population of foreign payees.

A very big thank you to the Benefits Protection Unit and Member Services staff with whom we partnered to complete this audit.

**NOTED AND APPROVED**

_____        **Date:** <u>April 29, 2020</u>

Richard Bendall
*Chief Audit Executive*

**REPORT ISTRIBUTION**

| | | |
|---|---|---|
| *2020 Audit Committee* | *JJ Popowich* | *Sylvia Botros* |
| *Santos Kreimann* | *Bernie Buenaflor* | |

# LACERA

June 16, 2020

TO:          2020 Audit Committee
                 Gina V. Sanchez, Chair
                 Keith Knox, Vice Chair
                 Herman B. Santos, Secretary
                 Vivian H. Gray
                 David Green

                 Audit Committee Consultant
                 Rick Wentzel


FROM:      Richard Bendall
                 Chief Audit Executive

                 Leisha Collins
                 Principal Internal Auditor

FOR:        June 25, 2020 Audit Committee Meeting

**SUBJECT: Final Audit Plan Status Report - FYE June 30, 2020**

Attached is the final Audit Plan Status Report for the Fiscal Year ending June 30, 2020. This Report provides information on the FYE 2020 Audit Plan (Audit Plan), the assurance, consulting, and advisory projects completed, and other Internal Audit activities.

**BACKGROUND**

At the July 2019 meeting, the Committee approved the Audit Plan which consisted of forty-one (41) projects. One unplanned project that required a significant amount of Internal Audit resources, in the first half of this fiscal year, was the facilitation and oversight of the LA County Audit of LACERA's Administrative Operations (County Audit). As a result, at the March 2020 meeting, the Committee approved staff amendments to the Audit Plan, removing seven projects (based on risk and timing) from the plan and adding four more. Of the four projects added, one was the County Audit as well as a related Mobil Device Management Audit plus an Ethical Cultural Assessment. The last of the four projects added was the oversight of a Service Organization Controls (SOC) assessment by Plante Moran, due to the change in an actuarial practice for LACERA's administration of Other Post-Employment Benefits (OPEB).

Our final Audit Plan has 38 projects. There are 45-line items on the attached document, which includes, the seven (7) lined out removed projects, as approved by the Committee in March. Significant progress has been made in completing the 38 projects:

| Project Type | Completed Projects | Current In Progress | Postponed to FY 2021 | Total Projects in Audit Plan |
|---|---|---|---|---|
| Audit | 12 | 5 | 7 | 24 |
| Consulting | 10 | | | 10 |
| Admin/Organizational | 3 | 1 | | 4 |
| | | | | |
| Total Projects | 25 | 6 | 7 | 38 |

The Amended Audit Plan does not include the substantial amount of work that was performed by Internal Audit in the following areas listed below and indicated in more detail on page 4:

1. Reviewing and consulting on business process changes and workarounds developed during the COVID pandemic.
2. Consulting and analysis on IT-related Policies and Procedures, and assisting the Systems Division due to SOC requirements and COVID 19.
3. Coordinating organizational efforts in the development of an IT End-User Manual.
4. Updating and refining the recommendation follow-up process and additional review of the status of recommendations from the external audit report.
5. Assisting LACERA's External Financial Auditor with retrieving testing documentation, because of the lack of access to the LACERA office building during the COVID 19 pandemic.

The following report provides the status of each project, and a brief description of each project is provided in Exhibit A.

## AMENDED INTERNAL AUDIT PLAN FYE 2020

A description of each audit area is included in Exhibit A.

| Audit/Project | Project Type | Audit Assignment/ Vendor | Status |
|---|---|---|---|
| **MANAGEMENT, GOVERNANCE & COMPLIANCE** | | | |
| 1.   Business Continuity/Disaster Recovery | Consulting | TS, RB, GL | Completed |
| **2.   Mobile Device Management Controls Audit (NEW)** | Audit | SV | Report Issued 6/4/2020 |
| 3.   Contract Management System Audit | Audit | KT | Report Issued 6/15/2020 |
| 4.   Employee Overtime Audit | Audit | TS | Postponed to FYE 2021 |
| 5.   Strategic Planning/Budget Process | Consulting | RB, TS | Completed |
| 6.   LACERA Fraud & Ethics Hotline | Org | KT | Completed |
| **7.   LA County Audit Oversight (NEW)** | Consulting | LC, RB, CL | Completed |
| **8.   Ethical Culture Assessment Research (NEW)** | Audit | KT, RB, LC | Completed |
| 9.   Form 700 Compliance Audit | Audit | TS, RB | In Progress |
| 10.  Continuous Auditing Program (CAP) | Audit | NA, GT | Completed |
| 11.  Timecard Review | Audit | TS | Report Issued 11/22/2019 |
| 12.  Corporate Credit Card Audit | Audit | KT, NA | In Progress |
| 13.  Privacy Audit Reco Coordination | Consulting | TS | Completed |
| 14.  Compliance Committee | Consulting | CL, RB | Completed |
| 15.  Strategic Goals Team Participation | Consulting | LC, RB | Completed |
| 16.  Quality Assurance Improvement Program | Admin | CL RB, LC | Completed |
| 17.  Risk Assessment – FYE 2021 | Admin | LC, RB | Completed |
| 18.  Internal Audit Operations Guide Update | Admin | LC, RB, CL | In Progress |
| ~~19.  Fiduciary Review~~ | Consulting | | Removed |
| ~~20.  Inventory Process Consulting~~ | Consulting | | Postponed to FYE 2021 |
| **BENEFITS ADMINISTRATION** | | | |
| ~~21.  Account Settlement Collection Audit~~ | Audit | | **Postponed to FY 2021** |
| 22.  Benefits' Exception Report Audit | Audit | SV | Report Issued 11/22/2019 |
| 23.  Quality Assurance Operations Review | Audit | KT | Postponed to FYE 2021 |
| 24.  Member Benefits Calculation Audit | Audit | NA | Postponed to FYE 2021 |
| 25.  Member Authentication Process | Consulting | GL, GT | Completed |
| 26.  Death Legal Process Audit | Audit | NA | In Progress |
| 27.  Foreign Payee Audit | Audit | NA | Report Issued 4/29/2020 |
| ~~28.  Member Appeal Process Review~~ | Audit | | Removed |
| ~~29.  Member Call Center Monitoring Review~~ | Audit | | Removed |
| **INFORMATION SYSTEMS** | | | |
| 30.  External Penetration Testing | Audit | Clear Skies | Report Issued 6/15/2020 |
| 31.  Web Portal Review | Audit | Clear Skies | Completed |
| 32.  Database Review | Audit | SV,GL,GT | In Progress |
| **33.  SOC Readiness Assessment Oversight (NEW)** | Consulting | CL | Completed |
| 34.  Cyber SIEM Review | Audit | GT | Postponed to FYE 2021 |
| 35.  Privilege Access Review | Audit | GT,SV | Postponed to FYE 2021 |
| 36.  Third Party Data Security Review | Audit | SV | Postponed to FYE 2021 |
| ~~37.  Project Management Review~~ | Audit | | Removed |
| **FINANCIAL & INVESTMENT OPERATIONS** | | | |
| 38.  External Financial Audit - Oversight | Audit | PlanteMoran | Completed |
| 39.  THC RE Financial Audits - Oversight | Audit | External Audit | Completed |
| 40.  Real Estate Manager Reviews | Audit | External Audit | Completed |
| 41.  Accounts Payables Audit | Audit | GL | In Progress |
| 42.  Investments Due Diligence Review | Audit | KT | Postponed to FYE 2021 |
| 43.  Actuarial Services - Oversight | Consulting | SV | Completed |
| 44.  Custodial Bank Services | Consulting | TS | Completed |
| ~~45.  Investment Data Controls Review~~ | Audit | | Removed |

Highest priority of risk to organization and Audit or Consulting work

High Priority organizational risk and Auditor or Consulting/Assignment

The following are unplanned projects or additions to the Audit Plan that are in-progress or completed:

| Project | Project Type | Audit Assignment | Status |
|---|---|---|---|
| LA County Audit Oversight | Consulting | LC, RB, CL | At the request of the BOS, the LA County Auditor-Controller conducted an audit of LACERA's Administrative operations and issued an audit report in November 2019. IA provided oversight of the audit and currently tracks and reports to the Exec Office the status of recommendations. **This is a significant project that was added to the amended FYE 2020 Audit Plan that was approved at the April meeting.** |
| Mobile Device Management Controls Audit | Audit | SV | The procurement and tracking of wireless devices was identified as a high-risk area and was included in the LA County Audit Report. The audit report was issued in June 2020. **This is a significant project that was added to the amended FYE 2020 Audit Plan that was approved at the April meeting.** |
| Ethical Cultural Assessment Research | Audit | KT, RB, LC | At the request of the Audit Committee Chair, IA researched firms to conduct an Ethical Cultural Assessment and developed an action plan and timeline for this engagement. The audit engagement will be included in the FYE 2021 Audit Plan. **This is a significant project that was added to the amended FYE 2020 Audit Plan that was approved at the April meeting.** |
| SOC Readiness Assessment Oversight | Consulting | CL | As a result of the OPEB Plan restructure, Plante Moran (PM) will perform a Systems and Organization Change (SOC) audit over the controls related to OPEB data. The first phase of the engagement is a Readiness Assessment. Due to the complexity of this project and coordination among several key divisions, IA has taken on the role of project manager. The Readiness Assessment began in February 2020 and will continue through June 2020. **This is a significant project that was added to the amended FYE 2020 Audit Plan that was approved at the April meeting.** |
| Remote Workaround Consulting | Consulting | All Staff | IA has been consulting with various divisions on process changes and workarounds while staff work remotely due to the pandemic. Workarounds are tracked and monitored, and were incorporated into the IA annual risk assessment and audit planning for FYE 2021. |
| Consulting for IT-related Policies and Procedures | | | Internal audit has assisted the Exec Office in reviewing and assessing IT related policies and procedures as a result of changes to IT business operations, policies and procedures due to the pandemic and also in planning for the SOC engagement. |
| IT End-User Manual | Consulting | CL, KS | Internal audit is facilitating the group meetings and discussion in the development of the IT End-User Manual. |
| Updates and Revisions to Recommendation Follow-Up Process | Consulting | All Staff | Internal Audit is reviewing the implementation status of past recommendations and confirming the completeness of action plans. Additional review has been performed on the recommendations from the 2016 Privacy Audit, as well as recommendations from various IT Security Reviews, and staff has been continuing to meet with division managers to address recommendations that have remained outstanding for several years to ensure the adequacy of action plans. Additional reporting of outstanding recommendations will be discussed with the Executive Office and reported to the Audit Committee. |
| PM Assistance with Audit Testwork | Audit | NA | Due to the pandemic, PM is unable to perform audit work at the LACERA Office. To facilitate their audit testing, IA staff are retrieving file/data and providing the information to PM for their audit work. |
| Check Deposit Safe Keeping | Consulting | TS | Review of process for obtaining, recording, and safekeeping checks prior to deposit and/or distribution. |
| Assistance with Public Records Request | Consulting | RB, LC, CL | Assist the Exec office and Legal in obtaining documentation relating to PRAs. |
| OPA Contract Study with Benefits and Milliman | Consulting | SV | Participate in discussion with key division on OPA contract study relating to member benefits. |
| Outside Agency OPEB data request | Consulting | SV | Assisted key divisions in acquiring requested OPEB information for outside agency. |

The following are projects removed from the Audit Plan:

| Project | Project Type | Audit Assignment | Status |
|---|---|---|---|
| Fiduciary Review | Consulting | TS, RB | Postponing consideration of a fiduciary review/audit until FYE 2021 Audit Plan to allow boards and organization to adjust/settle in under the direction of the new CEO . |
| Inventory Process | Audit | NA, CL | Management is completing an organization-wide inventory.  The Procurement Policy was approved in November 2019 and management has made significant progress in developing desk procedures, which are on track for completion by February 2020.  A new audit of wireless devices has been added to the current Audit Plan, which includes a review of inventory procedures relating to these devices. |
| Account Settlement Process | Audit | SV | Management is in the process of implementing recommendations from Internal Audit's preliminary review completed in FYE 2019 and management is making significant process changes to strengthen internal controls.  IA will defer this audit until next fiscal year to allow management sufficient time to incorporate changes. |
| Project Management Review | Audit | RB, LC | We removed this audit due to the renewed organizational focus on IT development projects and alignment of resources and projects with the strategic direction and goals of the organization. |
| Members Appeal Process | Audit | TS | Audit replaced with higher risk audit project. IA will consider this audit for FYE 2021. |
| Members Call Center Monitoring Review | Audit | NA | Audit replaced with higher risk audit project. IA will consider this audit for FYE 2021. |
| Investment Data Controls | Audit | SV | Audit replaced with higher risk audit project. IA will consider this audit for FYE 2021. |

Exhibit A

## AUDIT PLAN FYE 2020

The following table provides a description of each audit area included in the FYE 2020 Audit Plan.

| | PROJECT | DESCRIPTION |
|---|---|---|
| | **MANAGEMENT, GOVERNANE & COMPLIANCE** | |
| 1. | Business Continuity/Disaster Recovery | Assist management in working with the consultant to reengineer and enhance LACERA's Business Continuity/Disaster Recovery Program. |
| 2. | Mobile Device Management Controls Audit (NEW) | Review of effectiveness and efficiency of policies and procedures relating to the procurement, tracking, and disposal of wireless devices.  This audit area was also identified in the LA County Audit of LACERA's Operations. |
| 3. | Contract Management System Audit | Review the efficiency of the Contract Management System and effectiveness of policies and procedures for tracking and monitoring contract compliance. |
| 4. | Employee Overtime Audit | Audit of employee overtime practices throughout the organization to assess if adequate policies and procedures have been established and are followed. |
| 5. | Strategic Planning/Budget Process | Review of Strategic Plan in relation to budget planning and development. |
| 6. | LACERA Fraud and Ethics Hotline | Reengineer LACERA's Fraud and Ethics Hotline to incorporate a more enhanced system for the reporting and tracking of cases. |
| 7. | LA County Audit Oversight (NEW) | LA County Auditor-Controller conducted an audit of LACERA at the request of the LA BOS.  IA provided oversight of the LA County Audit and tracks and reports to the Exec Office the status of recommendations. |
| 8. | Ethical Cultural Assessment Research (NEW) | At the request of the Audit Committee Chair, IA researched firms to conduct an Ethical Cultural Assessment. |
| 9. | Form 700 Compliance Audit | Audit of Form 700s to assess staff and board compliance. |
| 10. | Continuous Auditing Program (CAP) | Automated testing of LACERA's transactions and information systems. CAP provides continuous assurance in key areas of compliance and includes fraud detection audits. |
| 11. | Timecard Review | Review organization-wide timekeeping controls to assess the accuracy of time reported and effectiveness of controls. |
| 12. | Corporate Credit Card Audit | Audit credit card usage to verify compliance with LACERA's Corporate Credit Card Policy. |
| 13. | Privacy Audit Recommendation Coordination | Oversee and actively coordinate the implementation of the recommendations as stated in the external Privacy Audit Report. |
| 14. | Compliance Committee | Participate on the Compliance Program Steering Committee in developing a framework for LACERA's formal compliance program. |
| 15. | Strategic Goals Team Participation | Staff participate in cross-functional teams (formed in FY 2019) to assist in the completion of the organization's strategic goals. |
| 16. | Quality Assurance Improvement Program (QAIP) | The QAIP includes ongoing monitoring of IA performance, periodic internal and external assessments, and communication of results to key stakeholders. Internal Audit will continue to formalize the QAIP, which is a FYE 2019 and FYE 2020 goal. |
| 17. | Risk Assessment – FYE 2021 | On an annual basis, Internal Audit assesses risks and controls throughout the organization to plan for LACERA's overall audit needs and to develop the Audit Plan. A FYE 2020 goal is to review and refine the risk assessment process. |
| 18. | Internal Audit Operations Guide Update | Update Internal Audit's Operation Guide.  This is a FYE 2019 and FYE 2020 goal. |

| | | |
|---|---|---|
| 19. | Fiduciary Review | Internal Audit will spearhead the Fiduciary Review conducted by an independent third party.  The purpose is to assess how well LACERA is meeting its governance and oversight responsibilities as well as the effectiveness of its operations. |
| 20. | Inventory Process Consulting | Review the inventory control process for completeness and efficiency. |
| | **BENEFITS ADMINISTRATION** | |
| 21. | Account Settlement Collection (ASC) Audit | The ASC Process is the collection of member and/or beneficiary's funds owed to LACERA. The Audit will serve as follow-up of management's progress in addressing areas of concern and deficiency from the FY 2019 review. |
| 22. | Benefits' Exception Report Review | Review the process for generating, managing, and using Benefit Exception Reports to assess effectiveness and efficiency. |
| 23. | Quality Assurance (QA) Operations Audit | Review QA operations for auditing benefit transactions and reporting audit results. |
| 24. | Member Benefit Calculation Audit | Audit member benefit calculations (on a risk basis) for accuracy and completeness. |
| 25. | Member Authentication Process | Review the adequacy and appropriateness of processes relating to authenticating members' identities prior to providing member information. |
| 26. | Death Legal Process Audit | Review Benefits, Member Services, and Legal divisions' processes for tracking and processing member death and legal split cases. |
| 27. | Foreign Payee Audit | Periodic audit that confirms the living status of retirees living abroad. |
| 28. | Member Appeal Process Review | Audit the member appeals process to assess if appeals are tracked, monitored, and resolved in compliance with laws and/or policies and procedures. |
| 29. | Member Call Center Monitoring Review | Review the effectiveness and efficiency of call monitoring in Member Services and Retirement Heath Care. |
| | **INFORMATION SYSTEMS** | |
| 30. | External Penetration Testing | Annual External Network Penetration testing to assess the security of LACERA's network, including the internet accessible Member Portal. |
| 31. | Web Portal Review | Review application security controls and application code for compliance with best practice guidelines. |
| 32. | Database Review | Review Microsoft Access databases used throughout LACERA to facilitate member transactions and benefits processes. Assess management controls to prevent process disruptions in case a database fails. |
| 33. | SOC Readiness Assessment (NEW) | As a result of the OPEB Plan restructure, Plante Moran, must perform a Systems and Organization Change (SOC) attestation engagement of census data. The first phase of the engagement is a Readiness Assessment.  IA has taken on the responsibility of project manager and liaison between the key stakeholders and the audit firm. |
| 34. | Cyber Security Information & Event Management (SIEM) | Review SIEM processes to ensure good practices exist for analyzing log-event data used to monitor threats and facilitate timely incident response. |
| 35. | Privileged Access Review | Review the creation, monitoring, and maintenance of privileged access credentials for compliance with best practice guidelines |
| 36. | Third Party Data Security Review | Review processes in place that protect the confidentiality, integrity, and availability of LACERA's data transferred to third parties. |
| 37. | Project Management Review | Assess the implementation of LACERA systems to meet business objectives. |
| | **FINANCIAL & INVESTMENT OPERATIONS** | |
| 38. | External Financial Audit - Oversight | Internal Audit manages the relationship with LACERA's external financial auditors for the annual financial statement audit. |
| 39. | THC Real Estate Audits - Oversight | Internal Audit manages the relationship with the Real Estate external auditors who perform the real estate THC financial audits. |
| 40. | Real Estate Manager Reviews | External audit firms conduct Real Estate Manager contract compliance and operational reviews on an as-needed basis. |
| 41. | Accounts Payables Audit | Audit of accounts payables, including payment vouchers and ACH transactions for accuracy. |
| 42. | Investment Due Diligence Review | Review due diligence practices relating to all asset classes for efficiency and effectiveness. |

| 43. | Actuarial Services - Oversight | Internal Audit manages the relationship with the Actuarial Consultant and Auditor for services relating to actuarial projects. |
|---|---|---|
| 44. | Custodial Bank Services | Participating on a consulting basis with the Investments Office and FASD in operational improvements of custodial bank services. |
| 45. | Investment Data Controls Review | Review investment data controls to ensure confidential financial data is adequately protected. |

# L/.CERA

June 16, 2020

TO:     2020 Audit Committee
        Gina V. Sanchez, Chair
        Keith Knox, Vice Chair
        Herman B. Santos, Secretary
        Vivian H. Gray
        David Green

        Audit Committee Consultant
        Rick Wentzel

FROM:   Richard Bendall
        Chief Audit Executive

        Leisha Collins
        Principal Internal Auditor

FOR:    June 25, 2020 Audit Committee Meeting

SUBJECT: **FYE 2021 Risk Assessment and Audit Plan Development**

## BACKGROUND

In accordance with the Institute of Internal Auditor's *(IIA's) International Standards for the Professional practice of Internal Auditing (Standards)*, the Chief Audit Executive *(CAE)* establishes risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals. To remain in compliance with the *Standards*, as well as the Audit Committee Charter, Internal Audit develops an Internal Audit Plan *(Audit Plan)* each fiscal year.

The projects included in our Audit Plan are primarily identified through our on-going risk assessment process. This process includes keeping abreast of the concerns of the Audit Committee and Boards throughout the year, discussions with Executive Management, review of LACERA's Strategic Plan, and risk meetings with division managers and staff. Due to organizational and operational changes resulting from the COVID Pandemic and the associated risks, Internal Audit is refining the risk assessment process and development of the FYE 2021 Audit Plan. This extended process will ensure better alignment with organizational needs.

The attached presentation provides an overview of our process and development of the Audit Plan which we will provide to the Committee for approval at the August 2020 Audit Committee Meeting.

# Internal Audit Process

Annual Audit Planning

Audit Plan Execution

**01**

**02**

**03**

**04**

**05**

**06**

**AUDIT UNIVERSE**

DEFINE

**RISK ASSESSMENT**

ASSESS

**AUDIT PLAN**

DEVELOP & REVIEW

**PLANNING**

PLAN

**FIELDWORK & DOCUMENTATION**

EXECUTE

**REPORT TO AUDIT COMMITTEE**

REPORT & TRACK

# Internal Audit Process

| Annual Audit Planning | | | Audit Plan Execution | | |
|---|---|---|---|---|---|
| **AUDIT UNIVERSE** | **RISK ASSESSMENT** | **AUDIT PLAN** | **PLANNING** | **FIELDWORK & DOCUMENTATION** | **REPORT TO AUDIT COMMITTEE** |
| ▪ Evaluate current audit universe by utilizing multiple sources of information.<br>▪ Update audit universe to include added or removed audit ideas. | ▪ Perform risk assessment.<br>▪ Measure the risk of each areas identified in the audit universe and assign a risk rating (High, Medium, Low) | ▪ Establish a schedule of audits by process/area based on annual risk assessment and previous year's audit results.<br>▪ Determine staffing needs. | ▪ Audit engagement memo sent to all divisions being audited.<br>▪ Internal Audit meets with division/area management to review risks areas and determine audit scope. | ▪ Internal Audit performs audit.<br>▪ Findings reviewed with division/area management.<br>▪ Exit meeting held to finalize audit findings and review management's plan for remediation. | ▪ Complete audits reported to Audit Committee.<br>▪ Outstanding audit finding tracking report shared with Audit Committee.<br>▪ Status of annual audit plan presented to Audit Committee. |

**DEFINE**      **ASSESS**      **DEVELOP & REVIEW**      **PLAN**      **EXECUTE**      **REPORT & TRACK**

# Risk Assessment – Questionnaire

**QUESTIONS 9-12:**
9. Have there been any significant staffing changes in the past year? How did these staffing changes impact your division?
10. List new legislative mandates that have or will impact your division.
11. List new processes or significant changes to work functions established in your division within the past year. How has this impacted your division? Do you anticipate any significant changes in fiscal year 2020-2021?
12. Were workarounds developed during the pandemic for any of your critical business functions?

**QUESTIONS 1-8:**
1. What are the key objectives/goals of your division?
2. What are the most significant operational limitations that will prevent your division from accomplishing your divisional objectives?
3. Are there any 2020-2021 strategic goals tied to work processes within your division?
4. Review attachment A – Business Process Functions and add significant processes or procedures in your division that are missing. List your divisions' 5 most critical business processes/functions; additional discussion on each of these functions will be included in your risk meeting.
5. Are all your critical business processes addressed in your Business Continuity Plan?
6. Are there any delays or backlogs in processes performed in your division?
7. List significant processes or procedures in your division that are not documented with written procedures.
8. Are there any specific control weaknesses or areas where controls could be further enhanced through additional segregation of duties or levels of approval, etc.?
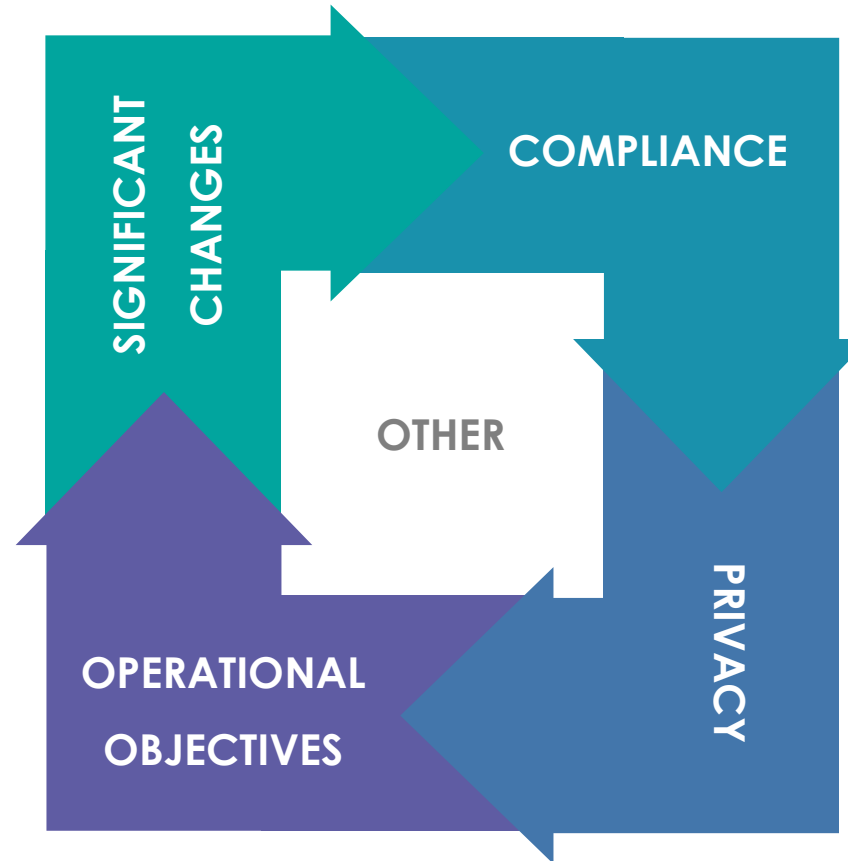
**QUESTIONS 13-19:**
13. Do you have divisional privacy policies or procedures?
14. Describe processes in your division where member data is sent outside of the organization.
15. Do any vendors you oversee have access to LACERA confidential data? If so, how do you ensure the data is adequately maintained and protected?
16. Describe processes in your division where member data is sent to other divisions within the organization, including the method the information is sent.
17. Do staff work remotely on sensitive information or member data?
18. If staff must transfer sensitive data beyond the parameters of their workstation, do you have divisional guidelines on how that data transfer should occur?
19. How is the importance of data privacy communicated to staff on an ongoing basis? Does your division have a clean desk policy?

**QUESTIONS 20-22:**
20. List areas of legal or regulatory compliance within your division and indicate if compliance is reported internally or externally, and frequency thereof.
21. Have contract been established with each vendor that is providing services through your division?
22. Describe your procedures for monitoring your vendor's compliance with contract terms.



SIGNIFICANT CHANGES

COMPLIANCE

OTHER

OPERATIONAL OBJECTIVES

PRIVACY

**QUESTIONS 23-25**
23. Describe frauds, privacy issues, or significant incidents in your division in the past year. How and to whom were these incidents reported?
24. What concerns you most about your division? What keeps you up at night?
25. How would you rate staff's understanding of internal controls and risks from 1 (low) to 5 (high).

4

# Risk Assessment – Universe



2020 AUDIT UNIVERSE - RISK ASSESSMENT

| REF | DIVISION | ORGANIZATION BRANCH | BUSINESS PROCESS/FUNCTION | AUDIT CYCLE | PRIOR AUDIT YEAR | PRIOR AUDIT RATING | ASSESSMENT SCORE | 2021 AUDIT PLAN | AUDIT PLAN | AUDIT PLAN | AUDIT PLAN |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Admin Services | Administration | Reception-Calls & Visitors | Periodic | | | Low | | | | |
| 2 | Admin Services | Administration | Check Distributions (IRIS, Admin, Payroll) | Periodic | | | Medium | | | | |
| 3 | Admin Services | Administration | Inventory Asset Management | Periodic | 2016 | | High | Yes | | | |
| 4 | Admin Services | Administration | Facilities Management | Periodic | | | Low | | Yes | | |
| 5 | Admin Services | Administration | Procurement Good & Services | Periodic | | | Medium | | | | |
| 6 | Admin Services | Administration | Business Continuity/Disaster Recovery | Annual | 2020 | | High | Yes | Yes | Yes | |
| 7 | Admin Services | Administration | Records Retention Management | Periodic | | | Low | | | | |
| 8 | Admin Services | Administration | Risk Management/Health & Safety | Periodic | | | Low | | | | |
| 9 | Admin Services | Administration | Ride Share Program | Periodic | | | Low | | | | |
| 10 | Admin Services | Administration | Contract Management | Periodic | 2020 | Opportunities for Improvement | Medium | | Yes | | |
| 11 | Admin Services | Administration | Renovations | Periodic | 2017 | | Low | | Yes | | |
| 12 | Admin Services | Administration | Budget Development & Monitoring | Annual | 2020 | | Medium | | | | |
| 13 | Admin Services | Administration | Documents Processing Center | Periodic | | | Medium | | | | |
| 14 | Admin Services | Administration | Mail Processing Services | Periodic | | | Low | | | | |
| | | | | | | | | | | | |
| 1 | Benefits | Operations | Interest Posting | | | | | | | | |
| 2 | Benefits | Operations | Withdrawals | | | | | | | | |
| 3 | Benefits | Operations | First Payment Agenda | | | | | | | | |
| 4 | Benefits | Operations | Benefits Exceptions Reporting | | 2020 | | | | | | |
| 5 | Benefits | Operations | Felony Forfeiture | | | | | | | | |
| 6 | Benefits | Operations | New Enrollment | | | | | | | | |
| 7 | Benefits | Operations | Open Window Plan Transfer | | | | | | | | |
| 8 | Benefits | Operations | Foreign Payees | | 2020 | | | | | | |
| 9 | Benefits | Operations | Temp Time Purchase | | | | | | | | |
| 10 | Benefits | Operations | Retroactive Payments | | | | | | | | |
| 11 | Benefits | Operations | Reciprocity | | | | | | | | |
| 12 | Benefits | Operations | Previous Service | | | | | | | | |
| 13 | Benefits | Operations | Terminations | | | | | | | | |
| 14 | Benefits | Operations | Disability Payroll | | | | | | | | |
| 15 | Benefits | Operations | Contract Rollovers | | | | | | | | |
| 16 | Benefits | Operations | Returned ADR | | | | | | | | |
| 17 | Benefits | Operations | Seamless Survivor | | | | | | | | |
| 18 | Benefits | Operations | Active Death Benefits | | 2020 | | | | | | |
| 19 | Benefits | Operations | Legal Splits | | | | | | | | |
| 20 | Benefits | Operations | Minor Survivor Continuance | | | | | | | | |
| 21 | Benefits | Operations | POA | | | | | | | | |
| 22 | Benefits | Operations | 1099/Taxes | | | | | | | | |
| 23 | Benefits | Operations | Discharge Cancellation | | | | | | | | |
| 24 | Benefits | Operations | 1014 Settlement | | | | | | | | |
| 25 | Benefits | Operations | Optional Membership | | | | | | | | |
| 26 | Benefits | Operations | Account Settlement Process | | 2019 | | | | | | |
| 27 | Benefits | Operations | Contribution Rate Change | | | | | | | | |
| 28 | Benefits | Operations | Outlawed Checks | | | | | | | | |

RISK UNIV | ADMIN | KEY | BENEFITS | COMM | DIS LIT | FASD | HR | INV | LEGAL | M …

# Risk Assessment – Division Level



| | FUNCTION/BUSINESS PROCESS | DESCRIPTION OF PROCESS | BCP CRITICAL (Per DM) | AUDIT CYCLE | PRIOR AUDIT YEAR | PRIOR AUDIT RATING | RISK ASSESSMENT RATING | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | | | | | | | FINANCIAL IMPACT | INTERNAL CONTROL | COMPLIANCE | REPUTATIONAL | EXECUTIVE/AC CONCERN | PANDEMIC IMPACT |
| 6 | Reception-Calls & Visitors | Reception section includes incoming and routing calls, visitor sign in, and parking validation. | X | Periodic | | | Low | Low | Low | Medium | Low | Low |
| 7 | Check Distributions (IRIS, Admin, Payroll) | Admin Services works with Benefits in the issuance of member checks including member withdrawals | X | Periodic | | | High | Medium | Medium | Medium | Medium | High |
| 8 | Inventory Asset Management | Management of Inventory and cycle counts, as well as disposal of obsolete items | X | Periodic | 2016 | | Medium | High | High | Medium | High | Medium |
| 9 | Facilities Management | | X | Periodic | | | Low | Low | Low | Medium | Low | Medium |
| 10 | Procurement Good & Services | Goods and Services for all divisions are reviewed and approved for purchased through Admin Services. | X | Periodic | | | High | Medium | Medium | High | Medium | Medium |
| 11 | Business Continuity/Disaster Recovery | Development of BCP, planning/oversight of BCP and DRS with Exec Office | | Annual | 2020 | | High | High | Medium | High | High | High |
| 12 | Records Retention Management | Records management and monitoring of records retention | | Periodic | | | Low | Low | Medium | Low | Low | Low |
| 13 | Risk Management/Health & Safety | Org risk management, purchase/maintenance LACERA insurance, and Health & Safety requirements | | Periodic | | | Low | Low | Medium | Low | Low | Low |
| 14 | Ride Share Program | Ride Share program is paid from LACERA budget. Staff reports are reviewed and approved for payment by Admin Secretary | | Periodic | | | Low | Low | Low | Low | Low | Low |
| 15 | Contract Management | CMS maintains contract records, except Investment and some Legal. Vendor Payments are approved against contracts. | | Periodic | 2020 | Opportunities for Improvement | Medium | Medium | Medium | Medium | Medium | Medium |
| 16 | Renovations | Oversight, planning, monitoring, of LACERA office renovations | | Periodic | 2017 | | Medium | Low | Low | Low | Low | Low |
| 17 | Budget Development & Monitoring | Development of budget, Reporting to Board, Approval and Mentoring/Reporting of Cost | | Annual | 2020 | | High | Medium | Low | High | High | Low |
| 18 | Documents Processing Center | Member Documents are received in DPC, scanned into MDL. DPC also performs printing projects. | | Periodic | | | Medium | Medium | Low | Low | Low | Medium |
| 19 | Mail Processing Services | Mail is received in Mail room and delivered throughout the organization by Mailroom staff | | Periodic | | | Low | Low | Low | Low | Low | Low |

# Audit Plan



## Fiscal Year 2019-2020

# LACERA



June 16, 2020

TO:        2020 Audit Committee
              Gina V. Sanchez, Chair
              Keith Knox, Vice Chair
              Herman B. Santos, Secretary
              Vivian H. Gray
              David Green

              Audit Committee Consultant
              Rick Wentzel

FROM:     Richard Bendall
              Chief Audit Executive

              Christina Logan
              Senior Internal Auditor

FOR:       June 25, 2020 Audit Committee Meeting

SUBJECT:  **Internal Audit's Quality Assurance and Improvement Program (QAIP)**

**Background**
The Institute of Internal Auditors (IIA) requires that chief audit executives develop and maintain a quality assurance and improvement program (QAIP). The QAIP must assess quality at both the broader internal audit activity and the individual audit engagement level. Internal assessments must be done on both a periodic and ongoing basis, and external assessments must be done at least every five years.

Internal Audit has always valued and strove to provide value-added work products and cohesive work environment. We already include many of the requirements established by the IIA *Standards* and industry best practices in our audits and administration. However, to further improve, Internal Audit had a goal to develop a more formalized QAIP. The results of our initial effort are summarized below.

**Periodic Self-Assessment**

The IIA provides a template to conduct a periodic self-assessment. The template is designed to assess conformance with the internal audit charter, the IIA's Definition of Internal Auditing, *Standards*, Code of Ethics, and to assess efficiency and effectiveness of internal audit in meeting the needs of its various stakeholders. The IIA also, provides the following rating scale:

| GC | Generally Conforms | PC | Partially Conforms |
|----|--------------------|----|--------------------|
| DNC | Does Not Conform | NA | Not Applicable |

Staff used this template and rating scale to conduct an annual self-assessment for fiscal year 2019-2020. The results of the self-assessment are below:

|   | Key Conformance Criteria | GC | PC | DNC | NA |
|---|--------------------------|----|----|-----|----|
| A | **Internal Audit Governance** | | | | |
|   | 1. Purpose, Authority, and Responsibility | ✓ | | | |
|   | 2. Independence & Objectivity | ✓ | | | |
|   | 3. Quality Assurance Program | ✓ | | | |
| B | **Internal Audit Staff** | | | | |
|   | 1. Proficiency | ✓ | | | |
| C | **Internal Audit Management** | | | | |
|   | 1. Planning | ✓ | | | |
|   | 2. Nature of Work | | ✓ | | |
| D | **Internal Audit Process** | | | | |
|   | 1. Operations Guide | ✓ | | | |
|   | 2. Engagement Planning | ✓ | | | |
|   | 3. Documenting Information | ✓ | | | |
|   | 4. Engagement Reporting | ✓ | | | |
|   | 5. Recommendation Follow-Up | ✓ | | | |

During fiscal year 2019-2020, Internal Audit undertook and completed the following key administrative projects to help improve our efficiency and effectiveness, and to provide clarity:

- Revised the Audit Report template to simplify the report, better clarify risks and findings.
- Revised and/or created additional audit templates for consistency – Entrance and Exit Meeting, Work Program, Preliminary Findings.
- Documented the internal audit process.
- Revised IA and AC Charters to align with IIA templates, peers, and each other.

As a result of this self-assessment and the revised Charters, Internal Audit will address the partially conforms regarding the "nature of our work" criteria by better incorporating governance, risk management, and controls assessments into our annual audit plan and engagements. We are currently reviewing, revising and documenting:

- The Policy and procedures for work paper documentation.
- The Preliminary Research and Analysis phase of the audit process.
- The Recommendation Follow-Up process.

We are also continuing to make improvements based on the results of the self-assessment and feedback received. Additional administrative projects we will be completing during upcoming fiscal year as a result of this QAIP include:

- Developing and having staff complete a Competent Auditor Self-Assessment to determine individual and division training needs and align training with goals.
- Developing and executing an On-Going Self-Monitoring program as required by the IIA.

**External Assessments**
The IIA requires an external assessment at least once every five years. The external assessment, like the periodic self-assessment, is designed to assess conformance with the internal audit charter, the IIA's Definition of Internal Auditing, *Standards*, Code of Ethics, and to assess efficiency and effectiveness of internal audit in meeting the needs of its various stakeholders.

Internal Audit's last external assessment was January 2016. The overall opinion from the assessment was that Internal Audit compliant with IIA's *Standards* and granted the division its highest rating of "generally conforms." The audit plan for this upcoming fiscal year includes having an external assessment performed.

# LACERA

June 16, 2020

TO:      2020 Audit Committee
         Gina V. Sanchez, Chair
         Keith Knox, Vice Chair
         Herman B. Santos, Secretary
         Vivian H. Gray
         David Green

         Audit Committee Consultant
         Rick Wentzel


FROM:    Richard Bendall
         Chief Audit Executive


         Leisha Collins
         Principal Internal Auditor

FOR:     June 25, 2020 Audit Committee Meeting


 SUBJECT:    **Internal Audit Goals Report**

The following Internal Audit Goal Report includes a status update on the completion of Fiscal Year End (FYE) 2020 goals. We will formulate and bring our FYE 2021 goals to your Committee in August. We welcome the opportunity for any questions, feedback or input from your Committee.


RB:LC


Attachment

# Internal Audit Goals – FYE 2020

**The following details the statuses of Internal Audit's goals for the period ending June 30, 2020:**

## Goal 1: Manage the completion of the FYE 2020 Audit Plan and develop a realistic risk-based Audit Plan for FYE 2021.

**Performance Measures:**
- Execute 80%* of the projects included in the FYE 20 Audit Plan by June 30, 2020. (*Note: 80% allows for flexibility due to changes in LACERA business practices and special requests.)
- Internal Audit will provide the FYE 2021 Audit Plan to the Audit Committee for approval at the August 2020 meeting.

**Status: Complete**

*A presentation of the final FYE 2020 Audit Plan to your Committee is included under separate cover for this June 25 meeting. An update on the risk assessment is also included for this meeting and staff will present the FYE 2021 Audit Plan to your Committee for approval at your August 2020 meeting.*

## Goal 2: Develop and implement audit performance and report writing standards

**Performance Measures:**

Internal Audit Operation Guide with the new audit performance and report writing standards by September 30, 2019.

**Status: Complete**

*We completed our Quality Assurance Improvement Program (QAIP) during this Fiscal Year, which is reported to your Committee under separate cover at this meeting. The QAIP process included the development of a revised audit reporting format which has been implemented as evidenced by recent reports provided to your Committee and reported under separate cover in this June 25 meeting. The QAIP process also resulted in the development of audit work paper and performance standards currently being finalized by staff.*

## Goal 3: Review and refine, as needed, the Internal Audit Risk Assessment process and present the revised process to the Audit Committee at the March 2020 meeting.

**Performance Measures:**

Presentation of risk assessment to the Audit Committee at the March 2020 meeting.

**Status: Complete**

*Staff did provide your Committee with an overview of the revised Risk Assessment process at your March meeting and has included a presentation providing your further information and insight to the process, under separate cover in this June 25 meeting. The final execution of the new risk assessment process will be presented to your Committee, in the form of our FYE 2021 Audit Plan, seeking your approval at your August meeting.*

**Goal 4: Monitor and measure Internal Audit efficiency using the internal evaluation of the Quality Assurance and Improvement Program (QAIP) and report results of the QAIP to the Audit Committee**

**Performance Measures:**

Internal Audit will complete a formal QAIP self-assessment in the first quarter of FYE 2020 and present a status update to the Audit Committee at the December 5, 2019 meeting.

**Status: Complete**

*While the exercise proved to be much bigger than anticipated and we did not complete it by your December 2019 meeting, we have now completed the QAIP and a presentation of the results is included under separate cover in this June 25 meeting.*

# LACERA

June 16, 2020

TO:        2020 Audit Committee
              Gina V. Sanchez, Chair
              Keith Knox, Vice Chair
              Herman B. Santos, Secretary
              Vivian H. Gray
              David Green

        Audit Committee Consultant
          Rick Wentzel

FROM:    Richard Bendall
         Chief Audit Executive

         Gabriel Tafoya
         Senior Internal Auditor

FOR:     June 25, 2020 Audit Committee Meeting

SUBJECT**:** **Recommendation Follow-Up Report**

Internal Audit reports to the Audit Committee at each meeting the status of all outstanding audit recommendations - **Attachment A.**

Since the March 2020 Audit Committee meeting, at which time there were twenty-five (25) outstanding audit recommendations:

- Twelve (12) were added, ten (10) in the Systems Division and two (2) in Administrative Services
- Two (2) were implemented, one (1) in Benefits, one (1) in the Systems Division.
- One (1) was removed from Benefits after Internal Audit validation for removal.

There are currently thirty-four (34) recommendations outstanding. A breakdown of outstanding recommendations by Division is represented in the following matrix.

| | Admin Services | Benefits | FASD | HR | Investments | Systems |
|---|---|---|---|---|---|---|
| **Beginning (25)** | 1 | 9 | 10 | 1 | 1 | 3 |
| **New** | 2 | 0 | 0 | 0 | 0 | 9 |
| **Implemented** | 0 | 1 | 0 | 0 | 0 | 1 |
| **Removed** | 0 | 1 | 0 | 0 | 0 | 0 |
| **Ending (34)** | 3 | 7 | 10 | 1 | 1 | 12 |

We are pleased to point out the age of outstanding recommendations is dropping significantly. There are now only six (6) outstanding recommendations over two years old, twenty-eight (28) outstanding less than two years with seventeen (17), of those related to recently issued audit reports and outstanding less than one year. We have noticed that management in all divisions are taking recommendation follow up very seriously and we are confident that all recommendations outstanding longer than two years will be implemented by the end of calendar year 2020.

| Internal Audit Issues Tracking | Open Findings | | | | | |
|---|---|---|---|---|---|---|
| | Total Open | Implemented | < 1 Year | > 1 Year | > 2 Years | > 3 Years |
| | 34 | 2 | 17 | 11 | 4 | 2 |

The chart below presents a graphical representation of outstanding recommendations by age in each division.
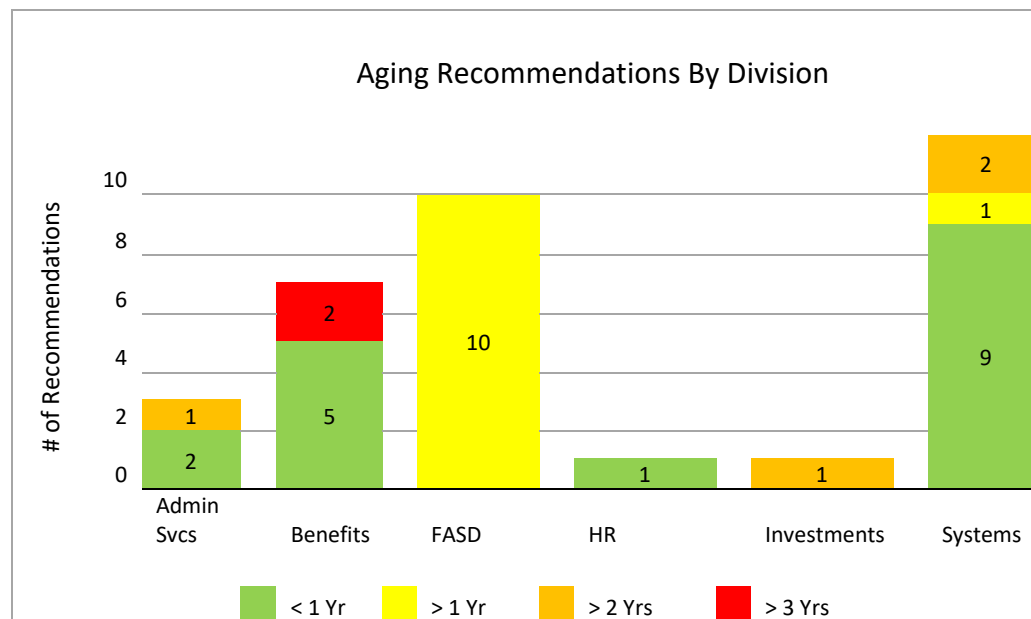


Internal Audit is working with management toward a goal that all recommendations are implemented within two years, with high-risk recommendations expedited.

We have also started to rate audit recommendations by risk for our newly published audit reports.  We have begun adding these risk ratings, for newly issued audit reports, to our Recommendation Follow-Up Report.

Internal Audit is continuing to offer support to all divisions in addressing their outstanding recommendations. Kudos to management and your Audit Committee for focusing on ensuring that audit recommendations are implemented timely.

Internal Audit and staff from the respective divisions will be present at your June 25 meeting to address your questions.

**IIA Standards**

The Institute of Internal Auditors' (IIA) Performance Standard #2500 pertains to monitoring the implementation progress of Internal Audit's recommendations made to Management. The Chief Audit Executive is required to establish and maintain a system to monitor the disposition of Management's corrective results and communicate those results to Executive Management and the Audit Committee.

During the audit process, Internal Audit, as well as external auditors (financial, fiduciary, actuarial, and IT), regularly identify areas where LACERA Management may implement changes to improve risk controls in its processes and Management provides action plans indicating how and when planned improvements will be made. These recommendations and action plans are included in each formal audit report. Additionally, Internal Audit makes recommendations and management identifies improvement plans during Internal Audit consulting assignments. All recommendations and management action plans are documented in Internal Audit's *Recommendation Follow-Up* database.

It is Internal Audit's responsibility to ensure that Management's action plans have been effectively implemented, or in the case of action plans that have yet to be implemented, to ensure that Management remains aware of the risks it has accepted by not taking action. In certain situations, if reported observations and recommendations are significant enough to require immediate action by Management, Internal Audit persistently monitors actions taken by Management until the observed risk is corrected.

It is not the responsibility of the Chief Audit Executive to resolve the risks identified during audit work. However, in accordance with IIA Performance Standard #2600, it is Internal Audit's responsibility to communicate the acceptance of risks when the Chief Audit Executive concludes that Management has accepted a level of risk that may be unacceptable to the organization.  As a result of this responsibility, Internal Audit communicates all pending *Management Action Plans* to LACERA's Executive Management and Audit Committee for resolution. In this manner, Internal Audit escalates unsatisfactory responses or lack of Management actions - including the assumption of risk - to the appropriate levels of Executive Management and the Audit Committee.

RB/gt

Attachments

| Project Name | Risk Area / Division | Finding | Risk Rating | Management Response | Responsible Party(s) | Responsible Division(s) | Original Implementation Date / Past Revision Dates | Current Status |
|---|---|---|---|---|---|---|---|---|
| | | | | **Administrative Services Division** | | | | |
| Contract Monitoring Program | Administrative Services Division<br><br>6/19/2018 | **Description of Finding:**<br>One area that can be improved is the database management system used to track invoice payments, which is separate from the CMS. The Administrative Services Division uses a Microsoft Access database to monitor the cumulative balances paid to a vendor. These balances are tracked outside of Microsoft Great Plains, LACERA's accounts payables system. Using Microsoft Access creates additional work, because Administrative Services staff must re-enter information from the invoices into an Access database after the information was already entered by Financial and Accounting Services Division ("FASD") staff. FASD staff enters invoice information into Microsoft Great Plains in order to pay invoices.<br><br>**Recommendation:**<br>Systems Division to work with Administrative Services to integrate Microsoft Great Plains with CMS where practical to minimize redundant work. | | **Original Management Response:**<br>Systems Division agrees with the recommendation and will work with Admin Services to integrate Microsoft Great Plains with CMS where practical to minimize redundant work. The estimated date for implementing this recommendation is October 31, 2018.<br><br>**Current Status:**<br>Administrative Services and Systems staff met and developed an implementation plan that will provide integration and reduced redundancy. Because of COVID-19 and new priorities, we expect to complete this project by 12/31/2020. | Kimberly Hines, Administrative Services Division<br><br>James Brekk, Systems Division<br><br>Ted Granger, FASD | Administrative Services Division<br><br>Systems Division | 10/31/2018<br>6/30/2020 | Pending<br><br>12/31/2020 |
| Contract Management Audit | Administrative Services Division<br><br>6/11/2020 | **Description of Finding:**<br>Strengthen controls in the administration of the current CMS application.<br><br>**Recommendation:**<br>1a. Ensure that contract managers perform periodic reviews, at least quarterly, of data in the CMS for which they are responsible and confirm the accuracy of the data.<br>1b. Complete the intended implementation of the current CMS system's functionality by activating the direct email function of reminders/prompts from the CMS to contract managers.<br>1c. Provide comprehensive training to all division managers and their delegated contract managers. | Medium | **Original Management Response:**<br>Administrative Services will:<br>1a. Implement a quarterly review process with contract managers to confirm that the data in the CMS is accurate.<br>1b. Implement/activate the CMS functionality related to automatically sending email reminders/prompts to contract managers.<br>1c. Provide comprehensive training to all division managers and their delegated contract managers.<br><br>Planned for completion by 12/31/2020. | Kimberly Hines, Administrative Services Division | Administrative Services Division<br><br>Systems Division | N/A | Pending<br><br>12/31/2020 |
| Contract Management Audit | Administrative Services Division<br><br>6/11/2020 | **Description of Finding:**<br>Our survey of contract managers also identified a desire to enhance the current CMS application. Beyond the additional functionality that is planned for the existing system, a number of contract managers expressed interest in a more comprehensive system which includes features such as automated workflows to facilitate contract development and approvals, facilitation of contract compliance monitoring, and a system which connects contracts to LACERA's budgeting and payment systems for tracking and monitoring of contracts.<br><br>**Recommendation:**<br>2. Administrative Services should evaluate the needs of the contract managers and the organization, and provide a written report to the Executive Office with recommendations to enhance the current CMS application or a recommendation to seek another product that will meet LACERA's needs. | Low | **Original Management Response:**<br>Administrative Services will evaluate the needs of the contract managers and the organization. A written report with recommendations will be provided to the Executive Office with recommendations to either enhance the current CMS application or to seek another product that will meet LACERA's needs. Planned for completion by 11/30/2020. | Kimberly Hines, Administrative Services Division<br><br>James Brekk, Systems Division | Administrative Services Division<br><br>Systems Division | N/A | Pending<br><br>11/30/2020 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Benefits Division** | | | | | | | | |
| Claims - Process Objectives, Risks, Controls, Process Flows, and Procedural Gaps | Benefits Division 4/12/2012 | **Description of Finding:** Benefit changes to member accounts made by staff (e.g., service credits, OASDI, PIA, member contributions, etc.) during First Payment do not require a secondary review or approval. These changes can significantly impact member benefits. As a best business practice, the duties of authorizing (initiating actions), approving, and processing member benefit transactions into Workspace and IRIS should be assigned in a manner that ensures adequate separation of duties exist. All Benefits staff have access to make these changes in Workspace and IRIS without a secondary electronic approver. First Payment procedures do not require a secondary review. In addition, QA audits only 25% of First Payments. There is a risk that staff may make erroneous or potentially fraudulent changes to member benefits that go undetected, resulting in on-going over or underpayments to the member. **Recommendation:** Benefits Management should work with Systems to restrict staff access to change member service credits, OASDI, PIA, contributions, etc. unless they have a specific business need. For staff that need access, Benefits Management should (or request Systems to) implement a secondary review or approval procedure when changes are made. If the above recommendations cannot be immediately implemented, Benefits Management should work with Systems to develop a report that identifies these changes and review the report to ensure each change is legitimate. | | **Original Management Response:** Benefits management will review the access list and work with Systems to limit access to those staff with a specific business need. However, implementing a secondary electronic approval for changes made to member service credits, OASDI, PIA, contributions, etc. may cause additional bottlenecks during the Agenda and First Payment process. Therefore, Benefits Management will work with Systems to develop reports that identify changes made between the Agenda and First Payment process. Supervisors will be instructed to review these reports before first payments are issued to ensure that all staff changes are legitimate. **Current Status:** A new Workspace feature has been implemented that mitigates the risk of staff making erroneous, potentially fraudulent changes to Member Benefits that may go undetected and may result in on-going over or under payments to members. A new work object was created for secondary review when critical changes to member accounts are made by staff using Workspace functions during critical first payment processing. The work object will be in the member's Work Roster and Events will have the details and the audit trail of the changes for review. | Bernie Buenaflor, Benefits Division  James Brekk, Systems Division | Benefits Division  Systems Division | 12/31/2012 3/7/2013 3/3/2014 2/17/2015 6/25/2015 10/29/2015 11/9/2015 6/22/2016 11/1/2016 11/8/2017 7/2/2018 10/31/2018 10/7/2019 12/31/2020 | Implemented 6/9/2020 |
| Previous service to contracts (QC/QA/CP) | Benefits Division 7/2/2013 | **Description of Finding:** In instances where OPA cases are passed along to other Benefits Division staff (for various reasons), we noted that the Benefits staff person is required to re-create the member's timeline in Workspace even though a timeline was already created by the staff who initially reviewed the member's account, and the member's work history did not change. **Recommendation:** When a members account needs to be re-reviewed by staff who did not perform the initial review, Management should evaluate the feasibility of requiring the secondary staff to rely on the initial timeline created. Additionally, Management may want to consider re-designing the process to have designated staff document timelines on the front end of the process before the cases are assigned to staff. Since timelines eventually get reviewed by QC Checkers, there are safeguards in place to help ensure inaccuracies are identified before the cost letters are sent. | | **Original Management Response:** Benefits will work with Quality Assurance to identify ways to 'certify' membership timelines and other work product so that they can be relied upon in completing future transactions for the same members. **Current Status:** LACERA has determined that this recommendation is best addressed through a comprehensive organization-wide strategy for addressing the integrity of member accounts. This strategy, currently known as account certification, will employ a structured, systems-based process for identifying, resolving, and documenting account discrepancies to ensure that staff responsible for transactions can reasonably rely upon account data without performing additional validation. Until such a strategy can be fully implemented, LACERA will continue to utilize redundant in-depth manual account analysis to address the risk that the account data used in member transactions is incorrect or incomplete. This recommendation was removed from this report as of 6/15/2020. Note: Internal Audit agrees that this is an efficiency recommendation, not an internal control issue. Until this can be automated as part of bigger comprehensive organizational plans, continuing the current practice is the conservative and more control based approach. Therefore, this recommendation will be removed and we will advise the Audit Committee accordingly at their June 25 meeting. | Bernie Buenaflor, Benefits Division | Benefits Division | 6/30/2014 6/26/2015 10/29/2015 6/22/2016 11/1/2016 7/2/2018 10/31/2018 6/18/2019 | Removed - Added to Organization Wide Strategy 6/15/2020 |
| Member Minor Survivor Compliance | Benefits Division 6/29/2016 | **Description of Finding:** We identified three instances where LACERA staff did not obtain one of the required documents prior to paying the minor survivor. Specifically, we noted: Two instances where the minor's account did not have a birth certificate on file. One instance where the minor's account did not have a claim form on file. We also noted that staff did not have desk procedures to determine which documents were required to determine the minor's eligibility. **Recommendation:** We recommend that the Benefits Division develop a procedural manual, provide staff additional training, and improve the review and approval process to ensure all required documents for minor survivor payees are valid and on file prior to payments being initiated. | | **Original Management Response:** The Benefits Division Process Management Group and the Special Benefits Services Section is currently developing the documented procedures and training material to address the recommendation to provide staff additional training, and improve the review and approval process to ensure all required documents for minor survivor payees are valid and on file. Procedures and training materials will be created and implemented by June 30, 2017, approximately. **Current Status:** Benefits anticipates the completion of desk procedures June 30, 2020, and completion of training on the new procedures to be completed by September 30, 2020. Systems estimates that the requested automation will be completed by September 30, 2020. The Systems Division will provide a timeline for completion. | Bernie Buenaflor, Benefits Division  James Brekk, Systems Division | Benefits Division  Systems Division | 6/30/2017 11/9/2017 7/2/2018 2/14/2019 10/31/2019 6/30/2020 | Pending 9/30/2020 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Duplicate Member Payments | Benefits Division 1/19/2017 | **Description of Finding:** To enhance the efficiency and effectiveness of the special payment approval process, we recommend that the Benefits Division work with the Systems Division to automate the remaining special payments processes that are currently approved manually. We also recommend that the Benefits and Systems Divisions work with Internal Audit during its development to help ensure that proper internal controls are designed into the automation process and that necessary data points are captured that will assist with post-transaction analytics and reporting.<br><br>**Recommendation:**<br>1. Benefits Division work with the Systems Division to automate the approval of those special payments processes where approvals are currently performed manually.<br><br>2. Benefits and Systems Divisions work with Internal Audit during its development to help ensure proper controls are designed into the automation process and that proper data points are captured that will assist with post-transaction analytics and reporting. | **Original Management Response:** Automating the approval process for special payments is feasible; however, special payments are initiated from multiple sources in Workspace. Each source will need to be analyzed and then specifications developed and tailored to each individual source. As such, the approval process would need to be implemented in a phased approach. Internal Audit will be included in the implementation process to ensure proper controls and reporting. There are some significant organizational goals that need to be completed before this modification can be addressed. It is estimated that determining the requirements and the level of effort can begin in the next fiscal year, July, 2017. The results of the requirement gathering will be reported to management by December 31, 2017, so that the project can be prioritized.<br><br>**Current Status:** Systems Division is in agreement with the current proposed date of implementation. Benefits currently uses a manual spreadsheet to control the processing and approval of special payments. Systems is developing an automated process, similar to the Withdrawal Workspace process, to help manage and control this process. This automated process should be in place by September 30, 2020. Systems will involve IA in the post-transaction analytics. | Bernie Buenaflor, Benefits Division<br><br>James Brekk, Systems Division | Benefits Division<br><br>Systems Division | 12/31/2017<br><br>10/31/2018<br>10/7/2019<br>6/30/2020 | Pending 9/30/2020 |
| Benefits Exception Report Audit | Benefits Division 11/22/2019 | **Description of Finding:** During our discussions with staff regarding their exception reports review procedures and as part of our report testing, we noted several instances where data on the exception reports lacked completeness, accuracy, and usefulness. Internal Audit performed a detailed review of records for at least one exception report in five of the six Account Integrity Services (AIS) and Special Benefits Services (SBS) teams, as the Benefits Protection Unit currently does not receive exception reports. Based on our analysis, we identified errors in each of the reports ranging from false positives, inaccurately classified records, missing time periods or unknown error types. Due to the completeness and accuracy issues as noted, in addition to the unknown error types printed on the reports, staff in AIS and SBS have determined that all records in an exception report would require validation, however time, resource constraints and competing priorities limited staffs' ability to consistently perform this function.<br><br>**Recommendation:**<br>Benefits and Systems management should collaboratively implement a consistent process to evaluate exception reports data for completeness, accuracy, and usefulness. The process should include steps to maintain an inventory of current reports and error types and identify reports that have inaccurate or irrelevant data. This will enhance staff's understanding of the content in the exception reports and ensure information that management and staff rely upon to make judgments regarding member accounts are meaningful and does not negatively impact LACERA's fiduciary duty to maintain the fund. | **Management Response:** Management agrees with the recommendation and will establish a system for routinely reviewing and, as needed, modifying systems-generated exception reports used by the Benefits Division. The Benefits Process Management Group will work in conjunction with LACERA's Compliance Office and Systems to address this challenge within the framework of LACERA's Compliance Program and LACERA's strategic vision. Management anticipates completing an evaluation of the key exception reports by June 30, 2020. Management also anticipates performing an ongoing analysis of exception reports as part of a future project to reengineer the application that produces the exception reports. The project is currently in the planning stage and is part of LACERA's long-term strategic plan.<br><br>**Current Status:** Process Management and Systems are implementing a new Exceptions Management System (EMS) which uses a three-pronged approach to address system data exceptions as follows:<br>1) Workspace work objects;<br>2) DB2 data warehouse; and<br>3) Member-centric Workspace Exceptions screens.<br>In this system, Process Management will manage the systematic review and import of existing and proposed exception reports into the new EMS. They will monitor the EMS and conduct periodic reviews to ensure the reports in the EMS remain accurate, relevant and effective. The anticipated production launch date for this new EMS system is December 31, 2020. | Bernie Buenaflor, Benefits Division<br><br>James Brekk, Systems Division | Benefits Division<br><br>Systems Division | 6/30/2020 | Pending 12/31/2020 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Benefits Exception Report Audit | Benefits Division 11/22/2019 | **Description of Finding:**<br>In addition to the exception reports that alert staff to errors in the automated batch jobs, other reports are routinely generated that identify certain instances where a member's account may need further staff review such as the "Missing Contributions," "Outlawed Checks" and "Deferred/Inactive Member" files. The "Missing Contributions" file contains members who could be underpaying their required contributions, while the "Outlawed Checks" file contains a listing of outstanding stale dated checks and the "Deferred/Inactive Member" file contains members who could potentially be required to take a minimum distribution for federal tax purposes. Per inquiry with staff in Account Settlement Unit, Internal Audit noted that due to competing priorities, false positive records as previously identified, time constraints, and limited staff resources, staff would often prioritize reviewing reports and processes that affect the on-time benefit payment for retired members over these reports. By doing so, there is an increased risk that significant errors are missed and not corrected which eventually become financially detrimental to our members. Internal Audit further noted, prior to our audit, the Benefits Division was already aware of the potential risk of not reviewing these reports and had already begun separate special projects to address the underlying issues in lieu of focusing on validating records in the exception reports. The Process Management Group (PMG) in Benefits is currently managing these special projects.<br><br>**Recommendation:**<br>Benefits management should continue working with the PMG group to evaluate and refine the exceptions reports review process however, management should also consider developing a process that includes:<br><br>a. Identifying a complete population of key reports and documenting the purpose of each report.<br>b. Documenting LACERA's exposure to additional risks and liabilities associated with the information in those key reports.<br>c. Defining procedures to consistently validate the completeness and accuracy for those reports when changes occur to business rules or the law. | | **Management Response:**<br>Management agrees with the recommendation and will consider these factors as it establishes a system for managing the exception reports. Management anticipates completing this recommendation by June 30, 2020.<br><br>**Current Status:**<br>As detailed under 1) above, the new Exceptions Management System includes the continuous monitoring and periodic review of exception reports. Planned for completion by 12/31/2020. | Bernie Buenaflor, Benefits Division | Benefits Division | 6/30/2020 | Pending 12/31/2020 |
| Benefits Exception Report Audit | Benefits Division 11/22/2019 | **Description of Finding:**<br>The Report Control Center (RCC) is the Benefits process for managing the large volume of reports that automatically print throughout the month. Staff assigned to the RCC are responsible only for collecting and sorting the printed reports, distributing them to the appropriate staff for review, and filing the reports that staff signed off. During our walkthrough of the RCC process, we observed that hard copies of the reports for the current and prior fiscal years are stored in locked cabinets in the Benefits Division suite due to the sensitive member data contained in each report. We confirmed that staff generally keep the cabinets locked at all times, including during normal business hours, and only a select number of staff have access to the cabinet keys. While this practice ensures that visitors and other employees who are not authorized do not inadvertently access sensitive information, we noted however that older RCC reports were exposed to such risks during the archiving process. RCC reports when archived to the basement of the building or off-site to Iron Mountain are placed into boxes that are not further secured and removed by staff in Administrative Services or the vendor.<br><br>**Recommendation:**<br>Benefits management should review and establish retention cut-off dates in the Report Control Center (RCC) to ensure that reports are destroyed after a certain time period to mitigate any potential information security risks. Benefits should also perform an inventory of currently stored reports and destroy reports no longer needed. | | **Management Response:**<br>Management agrees with the recommendation and will enforce LACERA's document retention policies in the Report Control Center (RCC). Management has instructed staff to work with the Records and Information Management (RIM) Unit to compile an inventory of all stored reports by December 31, 2019 and destroy reports no longer needed by March 31, 2020.<br><br>**Current Status:**<br>As detailed under 1) above, the new Exceptions Management System will phase out the use of hard copy reports. In the meantime, Report Control will enforce LACERA's established records retention policies. Planned for completion by 12/31/2020. | Bernie Buenaflor, Benefits Division | Benefits Division | 3/31/2020 | Pending 12/31/2020 |

| Benefits Exception Report Audit | Benefits Division 11/22/2019 | **Description of Finding:**<br>To determine timely deletion of obsolete or invalid exception reports, Internal Audit requested a listing of all current, retired, and transferred staff in both the Account Integrity Services and Special Benefit Services groups and a list of all reports sent those individuals. We noted two employees, who retired from LACERA during the first quarter of 2019, were still listed as active recipients.<br><br>We noted a contributing factor for the error was the lack of documented policies and procedures for consistently reviewing exception report content, report recipients and notifying Systems when a report was obsolete or a user should stop receiving a report. Prior to our audit, the Benefits Division had recognized the need to develop procedures for cleaning up the high volume of exception reports sent to the Division and currently has plans to work with Systems to define an appropriate process going forward. We should also note that the two retired staff members Internal Audit identified have since been removed from the active recipient lists for those reports.<br><br>**Recommendation:**<br>Benefits and Systems management should implement a formal periodic review process to evaluate exception reports data and recipients and establish policies and procedures to delete obsolete exception reports and recipients. A formalized review process, policies and procedures would help ensure that reports continue to assist the business unit achieve its operational objectives, obsolete reports are deleted timely and recipients only receive reports commensurate with their job responsibilities. | | **Management Response:**<br>Management agrees with the recommendation and will consider these factors as it establishes a system for managing the exception reports. Management anticipates defining the review process, policy and procedures, as well as implementing this recommendation by June 30, 2020.<br><br>**Current Status:**<br>As described under 1) above, reports will be vetted and updated before input into the new EMS, and will be reviewed periodically thereafter. Planned for completion by 12/31/2020. | Bernie Buenaflor, Benefits Division | Benefits Division | 6/30/2020 | Pending 12/31/2020 |
|---|---|---|---|---|---|---|---|---|
| Benefits Exception Report Audit | Benefits Division 11/22/2019 | **Description of Finding:**<br>Internal Audit noted during our discussions as well as during our sample report testing, several instances where exception reports containing hundreds of pages of data as well as numerous cover pages automatically print. One report in particular contained over 450+ pages and was configured to print twice a month while another report that printed daily had a total of 69 pages of which 38 contained cover page type information such as report name, recipient and database name. Per inquiry with staff in the Report Control Center as well as other areas that receive automatically printed reports, we noted that Benefit's staff have dedicated portions of their day to ensure the printers had paper at all times and that all exception reports pages were collected and sorted. Furthermore, Systems helpdesk staff would often automatically replace the ink and toner for those printers on a set schedule.<br><br>**Recommendation:**<br>Benefits and Systems management should collaboratively work to determine if all hard copy reports can be limited to electronic copy and allow staff to print only the reports and/or pages of the report that are needed. | | **Management Response:**<br>Management agrees with the recommendation and will consider these factors as it establishes a system for managing the exception reports. Benefits management anticipates completing an evaluation of the hard copy exception reports and Systems management has confirmed it is ready to convert those reports to electronic copies at the direction of Benefits by June 30, 2020.<br><br>**Current Status:**<br>As detailed under 1) above, the new Exceptions Management System will phase out the use of hard copy reports and ensure that exceptions are handled as efficiently as possible. Planned for completion by 12/31/2020. | Bernie Buenaflor, Benefits Division | Benefits Division | 6/30/2020 | Pending 12/31/2020 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Financial Accounting Services Division (FASD)** | | | | | | | | |
| Board and Staff Education & Travel | Financial Accounting Services Division<br><br>6/20/2019 | **Description of Finding:**<br>Audit test work identified areas where travelers did not follow Policy and related payment processes: pre-approval of educational conference, lodging upgrades, reimbursement of meal per diems, and ground transportation.<br><br>**Recommendation 1:**<br>FASD management should assess the need to obtain missing documentation and/or recover amounts from travelers for noncompliant transactions that were identified during the audit. | | **Original Management Response:**<br>Management concurs with the recommendation. FASD management will have staff review the audit exceptions, and follow-up with travelers to obtain missing documentation and/or recover any amounts owed, as applicable, due to non-compliant transactions.<br><br>**Current Status:**<br>Staff is reviewing audit exceptions to determine amounts and documentation which can be obtained from travelers for noncompliant transactions. This recommendation is expected to be completed by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 1/31/2020 | Pending<br><br>9/30/2020 |
| Board and Staff Education & Travel | Financial Accounting Services Division<br><br>6/20/2019 | **Description of Finding:**<br>Audit test work identified areas where travelers did not follow Policy and related payment processes: pre-approval of educational conference, lodging upgrades, reimbursement of meal per diems, and ground transportation.<br><br>**Recommendation 3:**<br>Management should periodically provide training to the Boards and staff on the Policy to ensure travelers and approvers are aware and compliant with the Policy requirements. | | **Original Management Response:**<br>Management concurs with the recommendation. FASD will work with the Executive and Legal Offices to schedule Travel Policy training for the Boards and staff at least annually or when the Policy is revised.<br><br>**Current Status:**<br>This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation. Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 6/30/2020 | Pending<br><br>9/30/2020 |
| Board and Staff Education & Travel | Financial Accounting Services Division<br><br>6/20/2019 | **Description of Finding:**<br>Audit test work identified areas where travelers did not follow Policy and related payment processes: pre-approval of educational conference, lodging upgrades, reimbursement of meal per diems, and ground transportation.<br><br>**Recommendation 5:**<br>To be consistent with the section "Authorized Expenses" (705.02) of the Policy, that expenses should be "reasonable and necessary," Boards and management should:<br><br>a. Revise the Policy to reflect current economical transportation services, like public transportation, taxis, or ride-share services. The Policy should still require the traveler to provide written justification for using an upgraded ground transportation service if used.<br><br>b. Update the Policy to address if and when the use of an executive car service is acceptable. | | **Original Management Response:**<br>Management concurs with this recommendation. Management will bring the issue to the JOGC for further discussion.<br><br>**Current Status:**<br>This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation.<br>Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 1/31/2020 | Pending<br><br>9/30/2020 |
| Board and Staff Education & Travel | Financial Accounting Services Division<br><br>6/20/2019 | **Description of Finding:**<br>FASD does not have a complete physical or electronic file for each travel event but instead maintains several platforms of information; a binder with all approved conferences and related agendas, a corporate credit card database, and Great Plains, a financial and accounting software system. Not having a complete file for each travel event decreases the effectiveness of the review process, an operational risk. Furthermore, incomplete travel files makes it more difficult for FASD to provide accurate numbers on the Travel Reports.<br><br>**Recommendation 1:**<br>To improve the effectiveness and efficiency of FASD's review process, FASD should provide instructions for the Travel Expense Voucher (payment request), so travelers can provide a complete travel file. | | **Original Management Response:**<br>Management concurs with the recommendation. FASD will update the Travel Expense Voucher to include clear written instructions for completing the document.<br><br>**Current Status:**<br>This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation.<br>Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 6/30/2020 | Pending<br><br>9/30/2020 |

| Board and Staff Education & Travel | Financial Accounting Services Division 6/20/2019 | **Description of Finding:** FASD does not have a complete physical or electronic file for each travel event but instead maintains several platforms of information; a binder with all approved conferences and related agendas, a corporate credit card database, and Great Plains, a financial and accounting software system. Not having a complete file for each travel event decreases the effectiveness of the review process, an operational risk. Furthermore, incomplete travel files makes it more difficult for FASD to provide accurate numbers on the Travel Reports. **Recommendation 2:** To improve the effectiveness and efficiency of FASD's review process, FASD should work with the Systems Division and the Executive Office to explore solutions that would allow travelers to upload and allocate travel receipts, and that would allow FASD to review and store complete travel files in a central location. | | **Original Management Response:** Management concurs with the recommendation. FASD held preliminary discussions with the Systems Division and the Executive Office to evaluate the feasibility of implementing a travel receipt capture and storage tool. **Current Status:** This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation. Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 6/30/2020 | **Pending** 9/30/2020 |
|---|---|---|---|---|---|---|---|---|
| Board and Staff Education & Travel | Financial Accounting Services Division 6/20/2019 | **Description of Finding:** Quarterly Travel Reports did not accurately reflect the travel expenditures for a traveler's trip. In addition to the inaccuracies that Internal Audit identified, we learned from discussions with FASD, the Executive Board Assistants, and the Legal Office that the FY 2018 Quarterly Travel Reports were significantly revised for inaccurate reporting of travel expenditures before a public data request was fulfilled. Based on discussions with FASD, many of the inaccuracies in the Reports were caused by having a key member of FASD's Disbursements Unit out of the office for the majority of the year, and not having a complete travel file, as discussed in the prior section. **Recommendation 2:** To improve the accuracy of the Quarterly Travel Reports, FASD should instruct travelers on providing a complete travel file, and work with the Systems Division and the Executive Office to explore having traveler's upload and allocate travel receipts to a central location. | | **Original Management Response:** Management agrees with the recommendation. FASD will provide instructions for complete travel files to travelers. In addition, FASD held preliminary discussions with the Systems Division and the Executive Office to evaluate the feasibility of implementing a travel receipt capture and storage tool. **Current Status:** This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation. Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 6/30/2020 | **Pending** 9/30/2020 |
| Board and Staff Education & Travel | Financial Accounting Services Division 6/20/2019 | **Description of Finding:** The current Policy does not clearly address the definition of administrative travel, how administrative meetings should be categorized, or if administrative travel should count towards a Board member's annual conference limit. Staff excluded administrative travel from the annual conference limits. Staff consistently applied this interpretation to all Board members and all Travel Reports have reflected this interpretation since July 2014. However, during our audit, we noted stakeholders were unclear if staff's interpretation of the Policy was correct. The Policy should be revised to more clearly address "Administrative Travel." **Recommendation:** To strengthen the Policy, the Boards and management should revise the Policy to clarify "Administrative Travel" to define controls regarding when administrative travel is authorized, if there is a limit to administrative travel, and how administrative travel should be categorized for Board members. | | **Original Management Response:** Management concurs with this recommendation. Management will bring the issue to the JOGC for further discussion. **Current Status:** This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation. Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 1/31/2020 | **Pending** 9/30/2020 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Board and Staff Education & Travel | Financial Accounting Services Division<br><br>6/20/2019 | **Description of Finding:**<br>Per the Policy, local educational conferences are conferences where there is no common carrier travel and lodging is under $1,500, and these conferences should not be counted towards the annual 8/12 conference limit. We observed that it is difficult to categorize which conferences should be considered "local educational conferences", not subject to the 8/12 limit, as this determination needs to be made for each traveler's individual travel expenditures. We reviewed the 4th Quarter FY 2018 Travel Report, and noted that staff had categorized several trips as "local educational conferences" but these trips included either airfare or lodging was over $1,500.<br><br>**Recommendation:**<br>To ensure conferences are consistently and accurately categorized, conference limitations are applied, and to assist Board members in planning their educational conferences, Boards and management should revise the Policy to provide a standardized definition of "local educational conferences" – for example, limiting these to Los Angeles County, Southern California, or a set distance from LACERA. | | **Original Management Response:**<br>Management concurs with this recommendation. Management will bring the issue to the JOGC for further discussion.<br><br>**Current Status:**<br>This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation.<br>Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 1/31/2020 | Pending<br><br>9/30/2020 |
| Board and Staff Education & Travel | Financial Accounting Services Division<br><br>6/20/2019 | **Description of Finding:**<br>We reviewed industry best practices, compared other public pension funds' education and travel policies and if available, published travel reports, and recent media articles regarding travel by governmental agencies. In our assessment of the current Policy, we noted it does not have an overarching educational strategy that focuses on developing and improving key skills that fiduciaries generally need.<br><br>**Recommendation:**<br>To improve the effectiveness and adequacy of the Policy, Boards and management should:<br>**a.** Review the Clapman report's education policy for a template of best practices.<br><br>**b.** Consider adopting an organizational-wide educational strategy and incorporating the "Trustee (Fiduciary) Knowledge Self-Assessment." Texas Teacher Retirement System and CalSTRS have both hired a consultant to assess the organizations' requirements and preferences and to provide guidance in developing an effective educational strategy.<br><br>**c.** Consider working with LACERA's Training Coordinator to develop a process to create a stakeholder's educational plan, monitor the broader educational needs of the Board for in-house training opportunities, and review and evaluate educational conferences. | | **Original Management Response:**<br>Management concurs with this recommendation. Management will bring the issue to the JOGC for further discussion.<br><br>**Current Status:**<br>This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation. Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 1/1/2020 | Pending<br><br>9/30/2020 |
| Board and Staff Education & Travel | Financial Accounting Services Division<br><br>6/20/2019 | **Description of Finding:**<br>Internal Audit analyzed the costs of registration, airfare, and lodging, for the last four fiscal years to gain a better understanding of the increase in Board education travel expenditures. Based on the analysis, the cost of airfare has sharply increased, and we believe LACERA's airfare costs could be reasonably reduced. We observed from our testing that refundable tickets were purchased for some travel events. Since the current Policy does not address if or when purchasing refundable tickets is allowed, the purchases were not out of compliance with the Policy. However, since refundable tickets are often two to three times the cost of non-refundable tickets, it seems inconsistent with the Policy's general commentary on Attachment A of the Policy, "Travelers are encouraged to schedule travel in a way that minimizes LACERA's travel expenses." Additionally, we noted that prudent procurement practices, such as comparing prices among at least three airlines flying to the destination, modifying dates and times of travel, and prohibiting Board members from limiting their travel to one specific airline, are not encouraged or enforced.<br><br>**Recommendation:**<br>To reduce LACERA's total airfare costs, Boards and management should:<br>**a.** Re-evaluate the use of business class airfare.<br><br>**b.** Evaluate stronger enforcement of prudent procurement practices as described above, including prohibiting the purchase of refundable tickets. | | **Original Management Response:**<br>Management concurs with this recommendation. Management will bring the issue to the JOGC for further discussion.<br><br>**Current Status:**<br>This recommendation is on hold pending the outcome of the Mosaic review. The consultant' project began in October 2019 and will be presented in a Joint Board meeting in June 2020. Subsequent to Mosiac's presentation, Management will address this recommendation. Planned for completion by 9/30/2020. | Ted Granger, FASD | Financial Accounting Services Division | 1/31/2020 | Pending<br><br>9/30/2020 |
| **Human Resources Division** | | | | | | | | |

| Timekeeping Audit | Human Resources Division  11/22/2019 | **Description of Finding:**  LACERA does not have a standard set of timekeeping policies or procedures. Human Resources (HR) management is responsible for designing control activities through formal policies and procedures that are written, dated, and signed. It would reduce potential risks such as inaccurate hours being recorded in the eHR system, inaccurate pay codes used for leaves or absences, and most importantly, inaccurate payroll.  **Recommendation:**  HR should develop formal timekeeping policies and procedures to promote consistency and compliance within LACERA. This includes understanding which Los Angeles County human resources laws and policies are applicable to LACERA. | | **Original Management Response:**  Management agrees with the recommendations. Human Resources Division developed a draft timekeeping policy and procedures along with a draft guide to timesheet coding and submission that is pending release of the new employee handbook. The estimated completion date is March 31, 2020.  **Current Status:**  The revisions have been made and are under review to also include the recent events.  The final document will be available by July 31, 2020. | Annette Cleary, Human Resources Division | Human Resources Division | 3/31/2020 3/31/2020 | Pending 7/31/2020 |
|---|---|---|---|---|---|---|---|---|

# Audit Recommendations Follow Up

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | **Investments Division** | | | | |
| Securities Lending | Investments Division<br><br>5/30/2018 | **Description of Finding:**<br>In an April 2017 memorandum to the Board of Investments, management expressed the need to periodically rebid the securities lending program as a good measure.  It is good a practice to understand the fee implications of using third-party lending agents and the impact on program cost and performance. During our review, we observed  two  cases when  LACERA  incurred additional costs for using GSAL as a third-party lending agent.  Even though LACERA incurred additional costs for using  GSAL as  a third-party  lending  agent, it would be difficult to quantify  or contend that LACERA is better off using a single  lender over multiple third-party lenders. LACERA may benefit from un-bundling each SSB service offering and pricing it individually.  In doing so,  management  can understand the costs-benefits its of using  third-party agents, and determine the best course of action for LACERA and the program going forward.<br><br>**Recommendation:**<br>Investments Office to assess the fee implications of working with third-party agents to provide securities lending services. | | **Original Management Response:**<br>Subject to BOI approval, Staff anticipates issuing an RFP for securities lending services in fiscal year 2018/2019, and that search will include an assessment of all related fees, including for third-party agents.<br><br>**Current Status:**<br>The Investment Office discussed the securities lending program RFP at the June BOI meeting, and a decision had been reached in closed session.  Once this information is made public, we will close out the recommendation.  Planned for completion by 11/30/2020. | Jon Grabel, Investments Division | Investments Division | 6/30/2019<br><br>3/31/2019 | Pending<br><br>11/30/2020 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Systems Division** | | | | | | | | | | | |
| Data Backup/ Retention Testing | Systems Division 2/14/2018 | **Description of Finding:** Recent technology upgrades of desktops computers and server systems rely upon live interface to Cloud Services, operating and email systems.  Recovery of these services at a remote processing facility has not been tested in conjunction with recovery of LACERA's core membership system.  **Recommendation:** Perform a recovery exercise of mission critical operations at a remote location as soon as practical to validate recovery procedures and capture learnings for potential disruptions. | | **Original Management Response:** Mission critical membership payroll, accounting and investment data processing functions will be replicated offsite in a disaster recovery scenario during the fourth calendar quarter of 2018.  **Current Status:** Currently, fundamental systems can be recovered. The Boulder backup site is unchanged and communications can be established from the Mesa backup site location or hotel depending on needs.  Data Backup testing will depend on when social distancing eases/location resources re-open.  We will test at that time.   In the meantime, a plan will be documented by September 30, 2020. | James Brekk, Systems Division | Systems Division | 12/31/2018 7/31/2018 | Pending 9/30/2020 |
| Member Applications Change Control | Systems Division 10/30/2018 | **Description of Finding:** We noted that there were no management reports available for use to monitor or detect changes to application code deployed to the production system.  In a well-controlled Change Management environment, administrative reports are used to monitor the movement of application code changes thru development to final production status. These reports help ensure necessary testing, documentation, provisioning and authorizations occurred, and changes to systems are introduced in a controlled and coordinated manner.  Management has established segregation of responsibilities for application code changes and relies upon staff to follow established code development, testing and management approval review procedures prior to presenting application code changes to other responsible staff for promoting to production.  However, historically, due to staffing shortages, some staff have had the ability to develop and promote code into production potentially without management oversight. This situation presents a risk that erroneous or malicious code could be introduced into production without detection.  **Recommendation:** Systems Division management should develop a system generated report for monitoring changes in application code.  Management review of this report should ensure code changes deployed into production are appropriate and approved. | | **Original Management Response:** We plan to develop a system generated Deployment Monitoring Report that will identify any instances when code is deployed into production. Management plans to complete an analysis and evaluation to determine if feasible based on current project priorities and resources. This evaluation is planned for completion by the end of June 2019, and if feasible will be planned for implementation by the end of December 2019.  **Current Status:** Appropriate resources to complete a transition to a new deployment tool are planned to be hired in July, 2020.   We are currently interviewing candidates for this position.  Once the position is filled, we should be able to complete the recommended action within six months or sooner after hiring date.  Planned for completion by 12/31/2020.   The Systems Division indicated that if this can be completed earlier, it will be.  Internal Audit anticipates that this will be completed by September 30, 2020, so that we are in alignment with Plante Morans's SOC readiness recommendations. | James Brekk, Systems Division | Systems Division | 12/31/2019 6/30/2020 | Pending 12/31/2020 |
| Member Applications Change Control | Systems Division 10/30/2018 | **Description of Finding:** A formal policy does not exist to provide guidelines for granting staff administrator access and system management privileges.  **Recommendation:** The Systems Division management should develop a formal Administrator Access Policy that applies to staff who are granted "Administrator" access on LACERA's systems, and management of privileged group membership. | | **Original Management Response:** Systems Division management should develop a formal Administrator Access Policy that applies to staff who are granted "Administrator" access on LACERA's systems, and management of privileged group membership.  **Current Status:** Currently, we have provided the Systems division Roles policy to Internal Audit. The supplement policy titled "Privileged Access Policy" will address this recommendation for closure.  Planned for completion by 9/30/2020. | James Brekk, Systems Division | Systems Division | 6/30/2019 2/28/2020 | Pending 9/30/2020 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Mobile Device Management Controls | Systems Division 6/4/2020 | Description of Finding: LACERA currently has four (4) separate mobile device policies, with three (3) designated for staff (one iPad Policy and two versions of a cell phone policy) and one (1) general mobile device policy specifically for Trustees. After reviewing the policies, we determined the policies were incomplete, outdated and did not include the following: • Type of information or devices permitted to access organizational information including standards and criteria for mobile device security, issuance, and management. • Guidelines and standards defining the authorization, purchasing, maintenance, inventory process, and disposing of mobile devices.<br><br>Recommendation 1: 1. Systems Division management should develop a comprehensive and consolidated organizational mobile device management policy to be approved by the Executive Office. The policy should include the following: • Data classification or information security standards that govern the level of security settings configured on each device. • Device monitoring requirements that includes regular assessments of mobile devices for excessive, personal, reimbursable or exception usage. • Documented cost control monitoring and follow-up. • Device issuance, specification, configuration and returns standards that align with business need criteria and job-related duties and functions. | High | Original Management Response: Management agrees with the recommendation and plans to complete implementation by September 30, 2020. The Systems Division created a draft Wireless Policy and Procedures document in February 2020 in response to the LA County audit. The finalization of the policy and procedures has been delayed as the result of the COVID-19 pandemic; however, Systems will review that policy and include items from this recommendation. | James Brekk, Systems Division | Systems Division | N/A | Pending 9/30/2020 |
| Mobile Device Management Controls | Systems Division 6/4/2020 | **Description of Finding**: LACERA's Policy for Purchasing Goods and Services (Procurement Policy) states that the centralized procurement unit in Administrative Services is the Purchasing Agent for LACERA.<br><br>We obtained a listing of all devices purchased during the audit scope period from November 1, 2018 through December 31, 2019 which identified three (3) cell phones in October 2019. We determined the procurement of the three cell phones purchased for testing purposes were made through Procurement. The only variance from the Policy was that Systems took delivery of all three devices directly from the carrier, which is not the standard receiving process.<br><br>**Recommendation 2:** 2. Systems Division and Administrative Services Division management ensure mobile devices are purchased and received in compliance with the LACERA Procurement Policy and recorded by Administrative Services in Great Plains inventory prior to being delivered to the Systems Division. | Low | Original Management Response: Management agrees with the recommendation and both Administrative Services and the Systems Division assert that this recommendation has been implemented. All mobile device purchases by the Systems Division are made through Procurement in compliance with the Procurement Policy. | James Brekk, Systems Division | Systems Division | N/A | Implemented 5/30/2020 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Mobile Device Management Controls | Systems Division 6/4/2020 | **Description of Finding**: LACERA has over 270 mobile devices, consisting of 140 laptops, notebooks or netbooks, and 130 smartphones, tablets, and wireless hotspots. Administrative Services registers all laptops, notebooks, and netbooks in the Great Plains Fixed Asset Register. However, prior to October 2019, mobile phones and tablets were not recorded or tracked in Great Plains per prior Executive Office direction. Systems internally tracked those assets separately using excel spreadsheets.<br><br>Per review of Systems' internal listings, we noted Systems had not completed a physical inventory, including spare, vacant, or test devices. Our review further identified areas to strengthen segregation of duties and controls around the mobile device inventory process.<br><br>**Recommendation 3:**<br>3a. Systems Division management create a current mobile device master listing that includes all active, inactive, vacant, and test devices issued by LACERA. Systems work with Administrative Services to record all mobile devices in Great Plains.<br>3b. Administrative Services and Systems management develop and implement a control-based mobile device inventory process. The process should include:<br>• Require execution of a formalized and documented annual inventory that includes active, inactive, vacant, and test devices.<br>• Documented responsibility for mobile device inventory asset accountability and tracking, device master listing maintenance, asset reconciliations and verification counts. | High | **Original Management Response:** Management agrees with the recommendations and plans to complete implementation by December 31, 2020. The Systems Division plans to continue maintaining the mobile device master listing outside of Great Plains to ensure appropriate recording of device information such as inactive, vacant, and test statuses. However, Systems will work with Administrative Services to ensure changes to the master listing are timely updated in Great Plains by Administrative Services. | James Brekk, Systems Division | Systems Division | N/A | Pending 12/31/2020 |
| Mobile Device Management Controls | Systems Division 6/4/2020 | **Description of Finding**: LACERA does not register all organization issued mobile devices to the respective MDM tools. Specifically, we noted approximately 20 mobile phones or tablets were not registered to MaaS360, and only 21 of 138 laptops were registered to Intune.<br><br>**Recommendation 4:**<br>4. Systems Division management define the organizational mobile device management (MDM) registration policy to be approved by the Executive Office. This should include documented exceptions to the policy, if any, approved by the Executive Office. | Medium | **Original Management Response:** Management agrees with the recommendation and plans to complete implementation by October 31, 2020. Systems Division management will work with the Executive Office to define the appropriate organizational MDM registration policy for all devices including spare or test devices. | James Brekk, Systems Division | Systems Division | N/A | Pending 10/31/2020 |
| Mobile Device Management Controls | Systems Division 6/4/2020 | **Description of Finding**: We observed that Systems has six (6) different security configurations in the IBM MaaS360 tool; for example, a unique configuration for Board iPads, staff iPads, staff iPhones vs. test iPhones, etc. Generally, Systems Division management is also focused on security and while they may have created these configurations with specific intent, it was not defined and documented.<br><br>Further, we compared the settings against LACERA's Unsafe Computer Practices Policy, Federal standards as defined by the National Institute of Standards and Technology (NIST), and industry best practices. Our analysis determined that functions were not restricted within the various configurations to ensure compliance with LACERA's Unsafe Computer Practices Policy.<br><br>**Recommendation 5:**<br>5a. Systems management in conjunction with the Executive Office define organizational baseline mobile device management (MDM) usage and security configurations to strengthen device security. This should include limiting or restricting any high-risk functions with documented exceptions to the policy.<br>5b. Establish periodic review of policy settings to ensure they remain current with industry standards and best practices. | Medium | **Original Management Response:** Management agrees with these recommendations and plans to complete implementation by October 31, 2020. The Systems Division evaluates security considerations in all implementation decisions and will work with the Executive Office to ensure appropriate operations objectives are met during this process. | James Brekk, Systems Division | Systems Division | N/A | Pending 10/31/2020 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Mobile Device Management Controls | Systems Division<br><br>6/4/2020 | **Description of Finding**:<br>LACERA adopted a standard of using and deploying Apple devices for mobile use. However, we noted that this was an informal decision by the Executive Office that was not documented. Based on our analysis of System's wireless cellular list, we determined there were also sixteen (16) Android devices assigned to Systems staff and one Trustee in addition to their Apple devices. Systems management stated it was not the intention to include Android devices for mass deployment and those devices served testing and long-term evaluation purposes. However, we noted again that testing of these devices was informal without any documented purpose, plan or reporting of results, and was done without any formal Executive Office approval.<br>We verified six (6) individuals in the Systems Division were assigned more than one test device of the same type (e.g., two iPads) and often with the same wireless carrier and for an undetermined and extended period of time.<br>Further, we noted Trustees typically receive an iPad and a laptop. We determined, however, one Trustee had 5 mobile devices including two tablets, one of them a Samsung android tablet test device, two laptops, and an active wireless hotspot still assigned to them but related to a previously returned laptop.<br>**Recommendation 6:**<br>6a. Systems Division Management should formalize and obtain Executive Office approval of mobile device issuance standards for staff and trustees and any exceptions to those standards should be documented and approved by the Executive Office.<br>6b. Systems Division Management should formalize and obtain Executive Office approval of a procedure for testing mobile devices. | High | **Original Management Response:**<br>Management agrees with the recommendations and plans to complete implementation by October 31, 2020. The Systems Division will work with the Executive Office to define the mobile device issuance standards for staff, trustees, and test mobile devices. | James Brekk, Systems Division | Systems Division | N/A | Pending<br><br>10/31/2020 |
| Mobile Device Management Controls | Systems Division<br><br>6/4/2020 | **Description of Finding**:<br>There are currently four (4) separate mobile device policies, which are incomplete and outdated. The staff policies include an area for signature/user acknowledgment, but we determined it was not obtained in practice. Alternatively, the Systems Division maintains a separate Property Designation Form for end users to sign when taking possession of the device.<br><br>Systems provided the signed Property Designations Forms for our audit testing as evidence that users acknowledge and abide by LACERA's mobile device policies. We noted that the form only contains acknowledgment of the quantity and type of devices issued and does not include acknowledgement that the user has read and will abide by LACERA's policies. Further, we determined that these acknowledgements are only obtained the first time a person receives a mobile device. No further acknowledgment was obtained either annually or when a similar device was replaced for the same user.<br><br>**Recommendation 7:**<br>7. Systems Division management should improve the administrative process over mobile device acknowledgement and usage forms. The process should include the following:<br>• Inclusion of the Form in the comprehensive and consolidated Mobile Device Management Policy.<br>• Requirement that staff and Trustees re-sign a mobile device acknowledgement form annually and whenever provided a new device. | High | **Original Management Response:**<br>Management agrees with the recommendation and plans to complete implementation by October 31, 2020. | James Brekk, Systems Division | Systems Division | N/A | Pending<br><br>10/31/2020 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Mobile Device Management Controls | Systems Division 6/4/2020 | **Description of Finding**: We analyzed all wireless bills for 2019 and noted the organization had an average of 189 wireless service lines, of which approximately 87 or 46% had limited or zero usage. Specifically, 15 wireless lines had usage fewer than 30 minutes and 72 had zero usage during 2019. Further, we noted 40 of the 87 limited or zero usage lines (46%) were designated as vacant or belonged to former staff or Trustees.<br><br>In addition to limited or zero usage devices, we also reviewed the wireless bills for abnormal charges. Our review of the August 2019 billing cycle specifically identified abnormal international data roaming charges were incurred totaling $5,875. Appropriate documentation validating the costs and Executive Office approval for the additional charges was not retained.<br><br>**Recommendation 8:**<br>8. Systems Division management establish guidelines approved by the Executive Office over the management and monitoring of wireless lines. | High | **Original Management Response:** Management agrees with the recommendation and plans to complete implementation by September 30, 2020. The Systems Division has performed a reconciliation of wireless service lines in March 2020 to enhance documentation of some zero and limited usage lines as standby, backup, quick availability, and those maintained for legal holds. The finalization of further action items from the reconciliation has been delayed as the result of the COVID-19 pandemic; however, System's will complete those steps during implementation of this recommendation. | James Brekk, Systems Division | Systems Division | N/A | Pending 9/30/2020 |
| Mobile Device Management Controls | Systems Division 6/4/2020 | **Description of Finding**: To determine timely deactivation of wireless services and proper disposal of mobile devices, we examined the 2019 monthly wireless services bills for all carriers and inquired with staff regarding disposal procedures. We determined LACERA had approximately 40 wireless lines designated as "vacant" or belonged to former staff and Trustees who were no longer associated with LACERA for up to five (5) years. We further identified the following disposal procedures that required improvement:<br>• LACERA has not disposed of any old or obsolete tablets or smartphones since inception of the mobile device program.<br>• Formal documentation to validate that old or obsolete and devices returned by staff were appropriately reset to factory settings or the data was wiped is not maintained.<br>• A former Trustee's iPad is still considered outstanding according to the most recent Trustee inventory count performed by the Board Offices in December 2019.<br>• Former Trustees could purchase their LACERA issued iPad. However, documentation outlining the approval and process was not maintained.<br>**Recommendation 9:**<br>9. Systems Division management develop a formal procedure approved by the Executive Office over the deactivation, reassignment, disposal and/or sale of mobile devices taken out of service. Additionally, this procedure should include the following:<br>• A timeframe and methodology for the disposal of devices.<br>• Formal documentation to validate that old, obsolete devices are appropriately reset to factory settings and wiped with a copy provided to the end user and Administrative Services.<br>• An accurate inventory of out of service devices is maintained. | High | **Original Management Response:** Management agrees with the recommendation and plans to complete implementation by October 31, 2020. | James Brekk, Systems Division | Systems Division | N/A | Pending 10/31/2020 |
| Mobile Device Management Controls | Systems Division 6/4/2020 | **Description of Finding**: Internal Audit noted the default LACERA workstation configuration enables USB access on all workstations. Systems then deploys a separate Group Policy Object (GPO), that disables USB access to individual workstations. This process indicates that Systems must maintain a deny USB GPO list of 498 workstations and a more effective approach would be to change the default setting to disable USB access during configuration and deploy a GPO that enables USB access. This will reduce the USB GPO listing to only approved workstations and assist Systems with performing a periodic review of approved workstations. Further, we found that there is no requirement or process to ensure that only encrypted USB devices are used for LACERA business.<br><br>**Recommendation 10:**<br>10. Systems Division management strengthen the process for managing workstations that have USB access enabled. The process should include:<br>• A periodic review of USB enabled workstations to ensure such access is still appropriate.<br>• A periodic reconciliation of the deny USB access listing against Administrative Services Fixed Asset Register.<br>• Encryption required for USB devices connected to LACERA workstations. | Medium | **Original Management Response:** Management agrees with the recommendation and plans to complete implementation by October 31, 2020. | James Brekk, Systems Division | Systems Division | N/A | Pending 10/31/2020 |

**LACERA**

Documents not attached are exempt from disclosure under the California Public Records Act and other legal authority.


For further information, contact:
LACERA
Attention: Public Records Act Requests
300 N. Lake Ave., Suite 620
Pasadena, CA 91101

# LA CERA

June 16, 2020

TO:       2020 Audit Committee
               Gina V. Sanchez, Chair
               Keith Knox, Vice Chair
               Herman B. Santos, Secretary
               Vivian H. Gray
               David Green

               Audit Committee Consultant
               Rick Wentzel

FROM:     Richard Bendall
               Chief Audit Executive

               Kathryn Ton
               Senior Internal Auditor

FOR**:**      June 25, 2020 Audit Committee Meeting

**SUBJECT:   Real Estate Manager Reviews**

Internal Audit hired four audit firms to perform compliance and consulting reviews of LACERA's real estate investment managers (managers) on an as-needed basis. These engagements are designed to assist LACERA in determining if real estate managers are in compliance with specific provisions of their internal business controls and contractual business policies and procedures established under their Master Real Estate Investment Advisor Agreement. This memorandum is to inform the Committee of manager reviews completed since the March meeting.

KPM & Associates completed a debt investment program review of Barings, LLC and there were no significant issues. There were two findings related to the quarterly report disclosures, one finding related to the Manager Investment Plan (MIP), and one finding related to the manager's certification concerning financial contacts. The manager has provided an action plan to address the findings and recommendations.

Internal Audit plans to have external auditors conduct three to five manager compliance reviews on a five year cycle, unless significant issues arise requiring a review of a manager on a more frequent basis. Staff will continue to provide updates to the Committee regarding future manager audits.

RB:kt

# LACERA

June 16, 2020

TO:        2019 Audit Committee
                Gina V. Sanchez, Chair
                Keith Knox, Vice Chair
                Herman B. Santos, Secretary
                Vivian H. Gray
                David Green

                Audit Committee Consultant
                Rick Wentzel

FROM:      Richard Bendall
                Chief Audit Executive

                Gabriel Tafoya
                Senior Internal Auditor

                Nathan K. Amick
                Internal Auditor

FOR:       June 25, 2020 Audit Committee Meeting

**SUBJECT:   Continuous Auditing Program (CAP)**

Internal Audit performs its **Continuous Auditing Program** (CAP) throughout the year. We defined CAP as continuous audit testing for fraud and compliance incorporating data analytics as the primary auditing tool.

- *Fraud Testing* – Provides timely insight into fraud indicators
- *Compliance Testing* – Ensures compliance through testing transactional data against established internal control rules and transactional profiles (e.g., *960-Hour Limit Test*)

Our primary data analytics tool **Audit Command Language** (ACL) allows us to examine large data sets to uncover exceptions, anomalies, hidden patterns, unknown correlations, and to assist with the audit process. ACL gives us the ability to review every transaction, not just sampling, which enables a more efficient analysis on a greater scale.

The intention of CAP is to give Internal Audit and LACERA Management greater visibility into processes, activities, and transactions, while adding value by means of improved compliance, risk management, and the ability to achieve business goals.

Should any of our CAP testing identify a systematic breakdown of controls, the project would be elevated and a full audit would be performed. In such a case, the Audit Committee would be notified.

**COMPLETED CONTINUOUS AUDIT PROGRAM TESTS**
**For the period of 02/21/2020 through 06/11/2020**

| Project Name | Project Category | Completion Date |
|---|---|---|
| New Payees | Fraud | 06/12/2020 |
| Duplicate Vendor Payments | Fraud | 06/08/2020 |
| Pay Codes Testing | Compliance | 06/05/2020 |

The list below is a detail of the above completed and in progress projects including project name, purpose, methodology, coverage period, test results, and the frequency at which the tests are performed.

# Continuous Audit Program (CAP) Testing Summary

| FRAUD TESTING | | | | | | |
|---|---|---|---|---|---|---|
| **DIVISION** | **PROJECT NAME** | **PURPOSE** | **COVERAGE PERIOD** | **TEST FREQUENCY** | **METHODOLOGY** | **RESULTS** |
| Benefits Division | New Payees | Validate the eligibility of all new payees added to the LACERA retirement payroll. | 02/01/2020 to 06/01/2020 | Monthly | Traced all new payees, per the monthly payroll, to valid historical member data from LACERA and the plan sponsor. | No exceptions were noted. |
| FASD | Duplicate Vendor Payments | To identify Duplicate vendor payments | 01/01/2019 to 04/30/2020 | Annually | • Analyzed 100% of vendor invoice payments paid LACERA's accounting system using ACL<br>• Identified potential duplicate payments were further analyzed and validated to physical invoice payment support documentation.<br>• FASD staff and management were also consulted to further validate potential duplicate invoice payments as needed. | No exceptions were noted. |

| COMPLIANCE TESTING | | | | | | |
|---|---|---|---|---|---|---|
| **DIVISION** | **PROJECT NAME** | **PURPOSE** | **COVERAGE PERIOD** | **TEST FREQUENCY** | **METHODOLOGY** | **RESULTS** |
| Executive Division | Pay Codes Testing | To determine all paycodes used by plan sponsor are LACERA BOR approved. | 01/01/20 to 03/31/20 | Quarterly | Match the LACERA pay codes master listing against the Los Angeles County (LAC) Auditor-Controller's paycode file, to identify discrepancies. | No exceptions were noted. |

# LACERA

June 16, 2020

TO:       2020 Audit Committee
            Gina V. Sanchez, Chair
            Keith Knox, Vice Chair
            Herman B. Santos, Secretary
            Vivian H. Gray
            David Green

            Audit Committee Consultant
            Rick Wentzel

FROM:    Richard Bendall
            Chief Audit Executive

            Kathryn Ton
            Senior Internal Auditor

FOR:     June 25, 2020 Audit Committee Meeting

**SUBJECT:  Ethics Hotline Status Report**

The purpose of this memorandum is to provide the Committee with information on ethics cases handled by LACERA through the first half of 2020. Since November 2019, LACERA has worked externally with NAVEX Global's EthicsPoint for its ethics hotline reporting and case management needs.

To date, LACERA has received three case reports, two of which have been closed out and one of which is under investigation at this time.

| Issue Type | Count | Divisions Involved | Status |
|---|---|---|---|
| Accounting & Auditing Matters | 1 | Systems | In Process |
| Time Abuse | 1 | Legal | Closed |
| Violations of Policy | 1 | Systems | Closed |

Staff will continue to provide updates to the Committee on future reports.

RB:kt