

# IN PERSON & VIRTUAL BOARD MEETING



TO VIEW VIA WEB



TO PROVIDE PUBLIC COMMENT

Members of the public may address the Committee orally and in writing. To provide Public Comment, you should visit the above link and complete the request form by selecting whether you will provide oral or written comment from the options located under Options next to the Committee meeting.

**Attention:** If you have any questions, you may email [PublicComment@lacera.com](mailto:PublicComment@lacera.com). If you would like to make a public comment during the committee meeting, review the Public Comment instructions.

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

# AGENDA

A REGULAR 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, CA 91101

9:00 A.M., MONDAY, MARCH 18, 2024

*This meeting will be conducted by the Audit Committee and Board of Retirement and Board of Investments both in person and by teleconference under California Government Code Section 54953 (f).*

*Any person may view the meeting in person at LACERA's offices or online at <https://LACERA.com/leadership/board-meetings>.*

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

## COMMITTEE TRUSTEES:

Nancy Durazo, BOR Trustee  
Vivian Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman Santos, BOI Trustee  
Keith Knox, Ex-Officio

## AUDIT COMMITTEE CONSULTANT

Larry Jensen

- I. CALL TO ORDER
- II. PLEDGE OF ALLEGIANCE
- III. ELECTIONS OF OFFICERS (Election of Chair, Vice Chair, and Secretary)

IV. PROCEDURE FOR TELECONFERENCE MEETING ATTENDANCE UNDER AB 2449, California Government Code Section 54953 (f)

- A. Just Cause
- B. Action on Emergency Circumstance Requests
- C. Statement of Persons Present at Teleconference Locations

V. APPROVAL OF THE MINUTES

- A. Approval of the Minutes of the Regular Meeting of December 14, 2023

VI. PUBLIC COMMENT

(Members of the public may address the Committee orally and in writing. To provide Public Comment, you should visit <https://LACERA.com/leadership/board-meetings> and complete the request form by selecting whether you will provide oral or written comment from the options located under Options next to the Committee meeting.

If you select oral comment, we will contact you via email with information and instruction as to how to access the meeting as a speaker. You will have up to 3 minutes to address the Committee. Oral comment requests will be accepted up to the close of the Public Comment item on the agenda.

If you select written comment, please input your written public comment or documentation on the above link as soon as possible and up to the close of the meeting. Written comment will be made part of the official record of the meeting. If you would like to remain anonymous at the meeting without stating your name, please leave the name field blank in the request form. If you have any questions, you may email [PublicComment@lacera.com](mailto:PublicComment@lacera.com).)

VII. NON-CONSENT ITEMS

A. **Proposed 2024 Audit Committee Meeting Dates**

Recommendation as submitted by Richard P. Bendall, Chief Audit Executive: That the Committee review and approve the proposed 2024 Audit Committee meeting dates.

(Memo dated February 23, 2024)

B. **Internal Audit Proposed Fiscal Year 2024 – 2025 Budget Request**

Recommendation as submitted by Richard P. Bendall, Chief Audit Executive: That the Committee approve the Internal Audit Proposed Fiscal Year 2024 - 2025 Budget Request, and upon approval, direct staff to include it in LACERA's Administrative Budget for Board approval. (Memo dated March 6, 2024)

VII. NON-CONSENT ITEMS (Continued)

C. **Bank of America Wire Transfer Audit**

Recommendation as submitted by Nathan K. Amick, Senior Internal Auditor: That the Committee review and discuss the following engagement report and take the following action(s):

1. Accept and file report;
2. Instruct staff to forward report to Boards or Committees;
3. Make recommendations to the Boards or Committees regarding actions as may be required based on audit findings; and/or
4. Provide further instruction to staff.  
(Presentation) (Memo dated March 5, 2024)

D. **Procurement of Goods Audit**

Recommendation as submitted by Gabriel Tafoya, Senior Internal Auditor: That the Committee review and discuss the following engagement report to take the following action(s):

1. Accept and file report;
2. Instruct staff to forward report to Boards or Committees;
3. Make recommendations to the Boards or Committees regarding actions as may be required based on audit findings; and/or
4. Provide further instruction to staff.  
(Presentation) (Memo dated March 6, 2024)

VIII. REPORTS

A. **2024 Audit Committee Orientation**

Christina Logan, Principal Internal Auditor  
Nathan K. Amick, Senior Internal Auditor  
(Presentation) (Memo dated March 5, 2024)

B. **Annual Audit Planning for Fiscal Year 2024 - 2025**

Richard P. Bendall, Chief Audit Executive  
(Presentation) (Memo dated March 5, 2024)

VIII. REPORTS (Continued)

C. **Fiscal Year Ending 2024 Audit Plan Status Report**

Richard P. Bendall, Chief Audit Executive  
Nathan K. Amick, Senior Internal Auditor  
(Presentation) (Memo dated March 5, 2024)

D. **Management's Compliance Report**

Steven P. Rice, Chief Counsel  
Luis A. Lugo, Deputy Chief Executive Officer  
(For Information Only) (Memo dated March 4, 2024)

E. **Recommendation Follow-Up Report**

Nathan K. Amick, Senior Internal Auditor  
(For Information Only) (Memo dated March 5, 2024)

F. **Recommendation Follow-Up Sensitive Information Technology Areas**

Gabriel Tafoya, Senior Internal Auditor  
(For Information Only) (Memo dated March 6, 2024)

G. **Ethics Hotline Status Update**

Leisha E. Collins, Principal Internal Auditor  
(For Information Only) (Memo dated March 5, 2024)

H. **Internal Audit Staffing Activity Report**

Richard P. Bendall, Chief Audit Executive  
(For Information Only) (Memo dated March 5, 2024)

I. **Status of Other External Audits Not Conducted at the Discretion of Internal Audit**

Richard P. Bendall, Chief Audit Executive  
(Verbal Update)

IX. CONSULTANT COMMENTS

Larry Jensen, Audit Committee Consultant  
(Verbal Presentation)

X. ITEMS FOR STAFF REVIEW

(This item summarizes requests and suggestions by individual trustees during the meeting for consideration by staff. These requests and suggestions do not constitute approval or formal action by the Board, which can only be made separately by motion on an agenda item at a future meeting.)

XI. ITEMS FOR FUTURE AGENDAS

(This item provides an opportunity for trustees to identify items to be included on a future agenda as permitted under the Board's Regulations.)

XII. GOOD OF THE ORDER

(For Information Purposes Only)

XIII. EXECUTIVE SESSION

A. Potential Threats to Public Services or Facilities

(Pursuant to Subdivision (a) of California Government Code Section 54957)

Consultation with: LACERA Chief Executive Officer Santos H. Kreimann, Deputy Chief Executive Officer Luis Lugo, Chief, Executive Audit Executive, Richard P. Bendall, Principal Internal Auditor, Christina Logan, Information Technology Kathy Delino, Information Security Officer Chaitanya Errande, and Other LACERA Staff.

XIV. 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.***

Any documents subject to public disclosure that relate to an agenda item for an open session of the Committee, that are distributed to members of the Committee 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 Committee, at LACERA's offices at 300 North Lake Avenue, Suite 820, Pasadena, California during normal business hours from 9:00 a.m. to 5:00 p.m. Monday through Friday and will also be posted on [lacera.com](http://lacera.com) at the same time, [Board Meetings | LACERA](#).

***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](mailto:PublicComment@lacera.com), but no later than 48 hours prior to the time the meeting is to commence.***

MINUTES OF THE REGULAR 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, CA 91101

9:00 A.M., THURSDAY, DECEMBER 14, 2023

This meeting was conducted by the Audit Committee, Board of Investments, and Board of Retirement both in person and by teleconference under California Government Code Section 54953 e(f).

COMMITTEE TRUSTEES

PRESENT: Gina V. Sanchez, Acting Chair

Patrick L. Jones, Secretary

Elizabeth Ginsberg, Alternate Ex-Officio

Antonio Sanchez, Trustee

ABSENT: Onyx Jones, Chair

Keith Knox, Vice Chair

Jason E. Green, Trustee

Shawn R. Kehoe, Trustee

STAFF, ADVISORS AND PARTICIPANTS

Santos H. Kreimann, Chief Executive Officer

Luis A. Lugo, Deputy Chief Executive Officer

Laura Guglielmo, Assistant Executive Officer

JJ Popowich, Assistant Executive Officer

STAFF, ADVISORS, PARTICIPANTS (Continued)

Steven P. Rice, Chief Counsel

Jonathan Grabel, Chief Investment Officer

Ted Granger, Interim Chief Financial Officer

Carly Ntoya, Human Resources Director

Kathy Delino, Chief Information Technology Officer

Summy Voong, Information Technology Manager

Richard P. Bendall, Chief Audit Executive

Leisha E. Collins, Principal Internal Auditor

Christina Logan, Principal Internal Auditor

Nathan K. Amick, Senior Internal Auditor

George Lunde, Senior Internal Auditor

Larry Jensen, Audit and Risk Management Services

Plante & Moran, PLLC

Jean Young, Engagement Partner

Amanda Cronk, Engagement Principal

Sarah Pavelek, Engagement Partner

Jenny Trotta, Engagement Principal

Robert H. Griffin, Audit Committee Consultant

I. CALL TO ORDER

This meeting was called to order by Acting Chair Gina Sanchez at 9:02 a.m. in the Board Room of Gateway Plaza.

II. PLEDGE OF ALLEGIANCE

Mr. A. Sanchez led the Trustees and staff in reciting the Pledge of Allegiance.

III. PROCEDURE FOR TELECONFERENCE MEETING ATTENDANCE UNDER AB 2449

- A. Just Cause
- B. Action on Emergency Circumstance Requests
- C. Statement of Persons Present at Teleconference Locations

No requests were received for Just Cause (A) or Emergency Circumstances (B).

III. APPROVAL OF MINUTES

- A. Approval of the Minutes of the Regular Meeting of August 31, 2023

Trustee P. Jones made a motion, Trustee A. Sanchez seconded, to approve the minutes of the regular meeting of August 31, 2023. The motion passed by the following roll call vote:

Yes: P. Jones, A. Sanchez, G. Sanchez, Ginsberg

No: None

V. PUBLIC COMMENT

There were no requests from the public to speak.

VI. NON-CONSENT ITEMS

- A. **Los Angeles County's Compliance with Requirements for Rehired Retirees – Fiscal Year Ended June 30, 2023**

Recommendation as submitted by George Lunde, Senior Internal Auditor: That the Committee review and discuss the following engagement report and take the following action(s).

1. Accept and file;
2. Instruct staff to forward memo to Boards or Committees;

VI. NON-CONSENT ITEMS (Continued)

3. Make recommendations to the Boards or Committees regarding actions as may be required based on the engagement and/or
4. Provide further instruction to staff.  
(Memo dated November 27, 2023)

Mr. Lunde provided a brief presentation. Messrs. Bendall, Kreimann and Popowich were present to answer questions from the Committee.

Trustee P. Jones made a motion, Alternate Ex-Officio Ginsberg seconded, to accept and file the report. The motion passed by the following roll call vote:

Yes: P. Jones, A. Sanchez, G. Sanchez, Ginsberg

No: None

**B. Review of Chief Executive Officer's Credit Card Expenditures**

Recommendation as submitted by Gabriel Tafoya, Senior Internal Auditor: That the Committee review and discuss the engagement and take the following action(s):

1. Accept and file;
2. Instruct staff to forward memo to Boards or Committees;
3. Make recommendations to the Boards or Committees regarding actions as may be required based on the engagement; and/or
4. Provide further instruction to staff.  
(Memo dated November 15, 2023)

Ms. Collins provided a brief presentation and answered questions from the Committee.

Trustee P. Jones made a motion, Trustee A. Sanchez seconded, to accept and file the report. The motion passed by the following roll call vote:

Yes: P. Jones, A. Sanchez, G. Sanchez, Ginsberg

No: None

VI. NON-CONSENT ITEMS (Continued)

C. **Replacement Benefit Plan Process 415(b)**

Recommendation as submitted by George Lunde, Senior Internal Auditor: That the Committee review and discuss the engagement report and take the following action(s):

1. Accept and file report;
2. Instruct staff to forward report to Boards or Committees;
3. Make recommendations to the Boards or Committees regarding actions as may be required based on audit findings; and/or
4. Provide further instruction to staff.  
(Memo dated November 30, 2023)  
(Memo dated November 11, 2023/Attorney-Client Privileged/  
Confidential Memo)

Mr. Lunde provided a brief presentation. Mr. Bendall was present to answer questions from the Committee.

Trustee P. Jones made a motion, Trustee Ginsberg seconded, to accept and file the report. The motion passed by the following roll call vote:

Yes: P. Jones, A. Sanchez, G. Sanchez, Ginsberg

No: None

D. **Consulting on Internal Controls over Financial Reporting – Cash and Treasury**

Recommendation as submitted by Nathan K. Amick, Senior Internal Auditor: That the Committee review and discuss the engagement report and take the following action(s):

1. Accept and file report;
2. Instruct staff to forward report to Boards or Committees;
3. Make recommendations to the Boards or Committees regarding actions as may be required based on audit findings; and/or

VI. NON-CONSENT ITEMS (Continued)

4. Provide further instruction to staff.  
(Memo dated November 15, 2023)

Mr. Amick provided a brief presentation and answered questions from the Committee.

Trustee A. Sanchez made a motion, Trustee P. Jones seconded, to accept and file the report. This item was received and filed. The motion passed by the following roll call vote:

Yes: P. Jones, A. Sanchez, G. Sanchez, Ginsberg

No: None

E. **Audit Committee Consultant Interviews and Selection**

Recommendation as submitted Leisha E. Collins, Principal Internal Auditor: That the Committee interview candidates and select an Audit Committee Consultant and upon selection of Audit Committee Consultant, direct staff to negotiate a three-year agreement, with two-one-year extensions for consulting services to begin in January 2024. (Presentation) (Memo dated November 30, 2023)

Ms. Collins provided a brief presentation. Messrs. Bendall, Kreimann, Grabel, Granger, Rice were present to answer questions from the Committee.

Trustee P. Jones made a motion, Trustee Ginsberg seconded, to negotiate and execute a three-year agreement, with two one-year extensions for consulting services to begin in January 2024 with Larry Jenson, Audit and Risk Management Services, LLC. The motion passed by the following roll call vote:

Yes: P. Jones, A. Sanchez, G. Sanchez, Ginsberg

No: None

VI. NON-CONSENT ITEMS (Continued)

F. **Fiscal Year 2024 Internal Audit Plan Amendments**

Recommendation as submitted by Richard P. Bendall, Chief Audit Executive and Nathan K. Amick, Senior Internal Auditor: That the Committee review and discuss the engagement report. (Presentation) (Memo dated November 30, 2023)

Mr. Amick provided a brief presentation. Mr. Bendall was present to answer questions from the Committee.

Trustee A. Sanchez made a motion, Trustee Ginsberg seconded, to approve Amendments. The motion passed by the following roll call vote:

Yes: P. Jones, A. Sanchez, G. Sanchez, Ginsberg

No: None

G. **Audit Committee Annual Report to Boards**

Recommendation as submitted by Onyx Jones, Audit Committee Chair and Richard P. Bendall, Chief Audit Executive: The Audit Committee provide suggested revisions and/or approve the issuance of the Audit Committee Annual Report to the Boards and direct staff to issue the report to the boards at their respective January 2024 meetings. (Memo dated November 30, 2023)

Mr. Bendall was present to answer questions from the Committee.

Trustee P. Jones made a motion, Trustee Ginsberg seconded, staff's recommendation. The motion passed by the following roll call vote:

Yes: P. Jones, A. Sanchez, G. Sanchez, Ginsberg

No: None

VII. REPORTS

A. **Plante Moran Financial Audit Reports**

Nathan K. Amick, Senior Internal Auditor  
(Presentation) (Memo dated November 15, 2023)

Ms. Young and Ms. Cronk of Plante Moran provided a brief presentation addressed questions from the Committee. This item was received and filed.

B. **Ethics Hotline Status Report**

Richard P. Bendall, Chief Audit Executive  
Leisha E. Collins, Principal Internal Auditor  
(Presentation) (Memo dated November 30, 2023)

Ms. Collins provided a brief presentation. Messrs. Bendall and Griffin were present to answer questions from the Committee. This item was received and filed.

C. **Internal Audit Charter Assessment**

Christina Logan, Principal Internal Auditor  
(For Information Only) (Memo dated November 15, 2023)

This item was received and filed.

D. **Continuous Auditing Program (CAP)**

George Lunde, Senior Internal Auditor  
(For Information Only) (Memo dated November 16, 2023)

This item was received and filed.

E. **Recommendation Follow-Up**

Kristina Sun, Senior Internal Auditor  
(For Information Only) (Memo dated August 16, 2023)

This item was received and filed.

F. **Recommendation Follow-Up Sensitive Information Technology Areas**

Gabriel Tafoya, Senior Internal Auditor  
(For Information Only) (Memo dated August 15, 2023)

This item was received and filed.

VII. REPORTS

G. **Internal Audit Staffing Activity Report**

Richard P. Bendall, Chief Audit Executive

(For Information Only) (Memo dated November 27, 2023)

This item was received and filed.

H. **Status of Other External Audits not conducted at the Discretion of Internal Audit**

Richard P. Bendall, Chief Audit Executive

(Verbal Update)

This item was received and filed.

VIII. CONSULTANT COMMENTS

Robert H. Griffin,

Audit Committee Consultant

(Verbal Presentation)

Mr. Griffin provided comments to the Committee.

IX. ITEMS FOR STAFF REVIEW

(This item summarizes requests and suggestions by individual trustees during the meeting for consideration by staff. These requests and suggestions do not constitute approval or formal action by the Board, which can only be made separately by motion on an agenda item at a future meeting.)

X. ITEMS FOR FUTURE AGENDAS

(This item provides an opportunity for trustees to identify items to be included on a future agenda as permitted under the Board's Regulations.)

XI. GOOD OF THE ORDER

(For Information Purposes Only)

The Committee thanked staff for their work.

## XII. EXECUTIVE SESSION

- A. Potential Threats to Public Services or Facilities  
(Pursuant to Subdivision (a) of California Government Code Section 54957)

Consultation with Terry Olejnik, Colleague Partner, Jenny Trotta, Engagement Principal, Sarah Pavelek, Engagement Partner from Plante Moran, Richard P. Bendall, Chief Audit Executive, Santos H. Kreimann, Chief Executive Officer, Luis Lugo, Deputy Chief Executive Officer, Kathy Delino, Chief Information Technology Officer, Chaitanya Errande, Information Security Officer and other LACERA Staff.

There was nothing to report.

- B. Performance Evaluation – Chief Audit Executive Goals Report  
(Pursuant to Government Code Section 54957(b)(1)  
(FOR AUDIT COMMITTEE ONLY PER COUNTY SALARY ORDINANCE 6.127.040.S.1)

Title: Chief Audit Executive

The Committee met in Executive Session with staff with regards to the Chief Audit Executive's performance evaluation and goals report.

There was nothing to report.

## XII. ADJOURNMENT

There being no further business to come before the Committee, the meeting was adjourned at 11:54 a.m.



February 23, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Richard P. Bendall   
Chief Audit Executive

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Proposed 2024 Committee Meeting Dates**

**RECOMMENDATION**

The Audit Committee review and approve the proposed 2024 Audit Committee meeting dates.

**AUDIT COMMITTEE DATES:**

The current Audit Committee Charter (Attachment A) states that the Audit Committee will conduct “regular meetings at least four times per year, with the authority to convene additional meetings, as circumstances require. The time frame between Audit Committee meetings should not exceed four months.”

Internal Audit reviewed the Board Calendar (Attachment B) to ensure the proposed meeting dates do not currently conflict with any other board scheduled events. We are proposing the Audit Committee meet approximately once a quarter on the following days at 9am.

<b>Day</b>	<b>Date</b>
Thursday	June 20, 2024
Thursday	September 19, 2024
Thursday	December 12, 2024

**AUDIT COMMITTEE CALENDAR**

On page 3 of this memo, we have attached the Annual Audit Committee Calendar, which is based on the proposed four meetings. Internal Audit developed this calendar to provide trustees on the Committee visibility to what they can expect at each meeting during the year. We have included in the calendar the Committee's annual and reoccurring responsibilities, as defined in the Audit Committee Charter to ensure they are addressed.

**Attachments**

A: April 2021 Audit Committee Charter

B: Board Calendar

Proposed 2024 Committee Meeting Dates

February 23, 2024

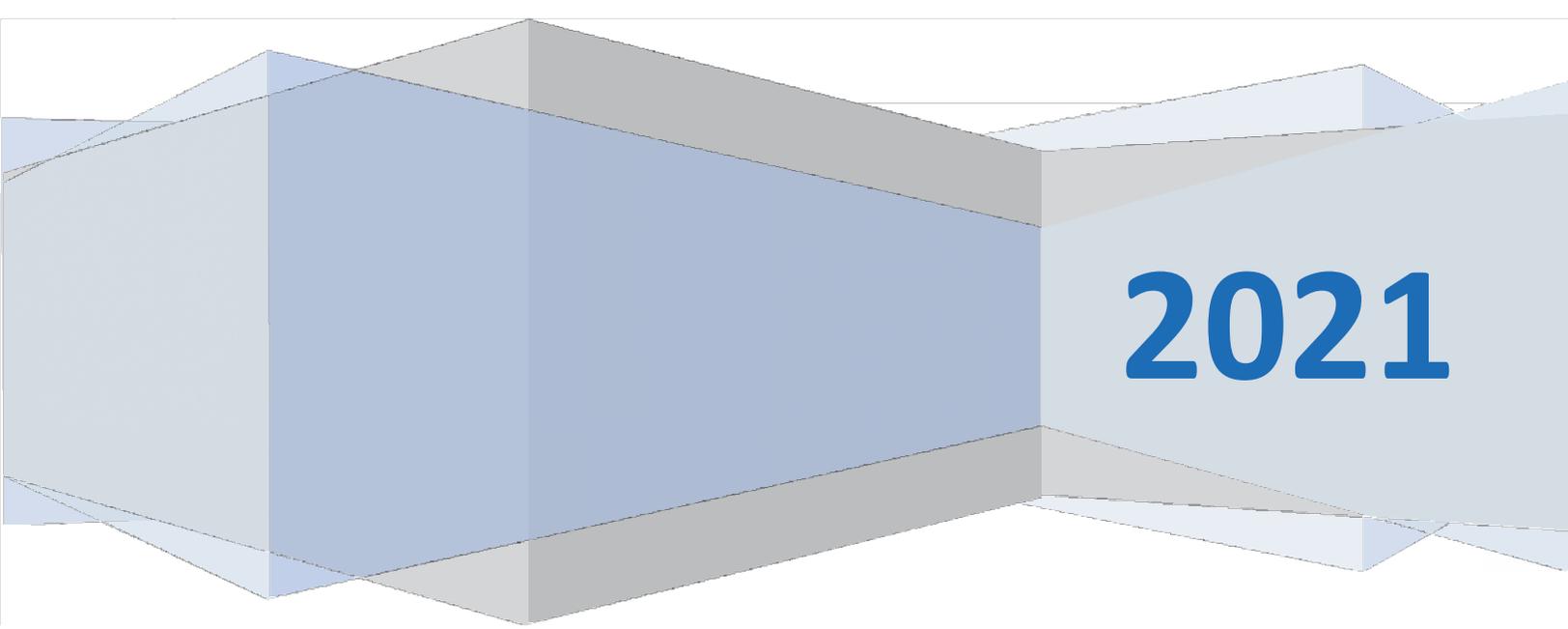
Page 3 of 3

2024 Annual Audit Committee Calendar						
Documentation	Ref to AC Charter	Frequency	Mar	June	Sept	Dec
Audit Engagement Reports	VII.A.2.a.	Every Meeting	C	X	X	X
Audit Plan Status Update	VII.A.1.d. & VII.A.2.c-d.	Every Meeting	C	X	X	X
Summary of Hotline Investigations	VII.D.3 & VII.E.2.b.	Every Meeting	C	X	X	X
Recommendation Follow-Up Reports	VII.A.2.b.	Every Meeting	C	X	X	X
Proposed Audit Plan and Budget	VII.A.1.c.	Annually	C			
Annual Risk Assessment	VII.A.1.a.	Annually		X		
Annual Audit Plan	VII.A.1.b.	Annually		X		
Presentation / memo by Financial Auditor detailing proposed scope of work and timing.	VII.B.2	Annually		X		
Internal Audit Charter	VII.A.3.a.	Annually		X		
Internal Audit Annual Performance Report	VII.A.3.b.-c.	Annually			X	
CAE Performance Evaluation	VII.A.4.b.-c.	Annually			X	
Ethics & Values Review	VII.D.1-3.	Annually			X	
Organizational Governance Review	VII.E.	Annually			X	
Compliance Memo from Legal Office	VII.E.4.c.	Annually	C			
Financial Statements, Correspondence, & Presentation	VII.C.1.-4.	Annually		X		X
Audit Committee Annual Performance Report	VII.F.1.	Annually				X
Audit Committee Charter	VII.F.4	Every 3rd year	Approved in 2021 Upcoming review 2024			
Approve the appointment and compensation of the External Financial Auditor	VII.B.1	Every 5th year**	Approved in 2023. Contract will expire 2027.			
Ensure IA has an external quality assessment performed every five years.	VII.A.3.d.	Every 5th year	Completed in 2022 Upcoming review 2027			
Provide an open avenue of communication between IA, all Professional Service Providers, Management, and the Boards.	VII.F.2	Continuous				
Approve the appointment & compensation of other Professional Service Providers, hired to perform non- financial statement audits, reviews or consulting, subject to limitations.	VII.B.2	As needed				
Review with Professional Service Providers, including the Financial Auditor, and Mgmt the results of the work performed, any findings & recommendations, Mngmt's responses, and actions taken to implement the audit recommendations.	VII.B.3	As needed				
Advise the Boards about any recommendations for the continuous improvement of the internal audit activity.	VII.A.3.e.	As needed				
Make recommendations to both Boards regarding the appointment, discipline, and/or dismissal, of the CAE, which will be addressed by the Boards in a joint meeting.	VII.A.4.a.	As needed				
Perform other activities related to this Charter as requested by the Boards.	VII.F.3	As needed				

C = completed, X = pending

# Audit Committee Charter

**April 2021**



**2021**



**AUDIT COMMITTEE CHARTER**

**Table of Contents**

**I. CHARTER .....2**

**II. PURPOSE AND ASSIGNED FIDUCIARY OVERSIGHT DUTIES.....2**

**III. PRINCIPLES OF THE AUDIT COMMITTEE ..... 2**

**IV. AUTHORITY .....3**

**V. AUDIT COMMITTEE COMPOSITION AND CONSULTANT..... 3**

**VI. AUDIT COMMITTEE MEETINGS .....4**

**VII. RESPONSIBILITIES .....5**

**VIII. APPROVAL.....9**



## 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
- F. Audit Committee and Internal Audit Budget

### 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.

#### **V. AUDIT COMMITTEE COMPOSITION AND CONSULTANT**

The Audit Committee will consist of seven members: three elected annually from each Board and the ex-officio member of both Boards, the Los Angeles County Treasurer. If any elected Audit Committee member leaves Board service or resigns from the Audit Committee prior to the completion of his or her term, the Board of the departing member, will elect a new Audit Committee member at the next regularly scheduled Board meeting.

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 Chair, 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.

All meetings of the Audit Committee shall be as noticed as joint meetings with the Board of Retirement and Board of Investments to allow for participation of all trustees in open and closed session Audit Committee discussions, provided that non-committee trustees may not make or second motions or vote and provided further that closed sessions to discuss the CAE's annual assessment and the Committee's recommendation to the Boards regarding the appointment, discipline, dismissal, and/or removal of the CAE shall be noticed for attendance by Committee members only.

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 and also published on the LACERA website, [lacera.com](http://lacera.com). 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 the seven-member Audit Committee, 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. 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 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.
4. Resolve any significant disagreements regarding risks, findings and/or compensation between management and Professional Service Providers

#### **C. Financial Reporting Process**

The Audit Committee is responsible for oversight of the independent audit of LACERA's financial statements, 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. Audit Committee and Internal Audit Budget**

LACERA will provide appropriate funding, as determined by the Audit Committee, for compensation to the Financial Auditor, to any Professional Service Provider that the Audit Committee chooses to engage, and for payment of ordinary administrative expenses of the Audit Committee that are necessary or appropriate in carrying out its duties.

**G. 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 April 23, 2021, and approved by the Board of Retirement on July 7, 2021, and the Board of Investments on July 14, 2021. This Charter is thereby effective July 14, 2021 and is hereby signed by the following persons who have authority and responsibilities under this Charter.

*Joseph Kelly**July 19, 2021*


---

**Joseph Kelly**  
Chair, Audit Committee

---

**Date**

*Keith Knox**July 19, 2021*


---

**Keith Knox**  
Chair, Board of Investments

---

**Date**

*Alan Bernstein**July 19, 2021*


---

**Alan Bernstein**  
Chair, Board of Retirement

---

**Date**

March

2024

SUN	MON	TUE	WED	THU	FRI	SAT
25	26	27	28	29	1	2
						CALAPRS General Assembly – Rancho Mirage – March 2 - 5
3	4	5	6	7	8	9
CALAPRS General Assembly – Rancho Mirage March 2 - 5			BOR & Committees IFEBP Investments Institute – Rancho Mirage, CA - March 6-7			
	CII Spring Conference – Washington, DC - March 4 –6			PPI Winter Roundtable – Napa, CA March 6-8		
10	11	12	13	14	15	16
			BOI & Committees			
		AHIP Medicare, Medicaid, Duals Forum – Baltimore, MD – March 12-14				
17	18	19	20	21	22	23
	Audit Committee			PREA Spring Conference – Nashville, TN – March 21-22		
			NASP Day of Education in Private Equity Marina Del Rey – March 20 - 21			
24	25	26	27	28	29	30
	Cesar Chavez Day				Good Friday	
31	1	2	3	4	5	6
Easter Sunday						

# June

2024

SUN	MON	TUE	WED	THU	FRI	SAT
26	27	28	29	30	31	1
2	3	4	5	6	7	8
<b>BOR &amp; Committees</b>						
9	10	11	12	13	14	15
<b>BOI &amp; Committees</b>						
		NASP Conference – Atlanta, GA - June 10-12				
		AHIP Conference – Las Vegas, NV - June 11-13				
16	17	18	19	20	21	22
			<b>Juneteenth</b>	<b>Audit Committee</b>		
23	24	25	26	27	28	29
		IFEBP Trustee Institute (Level I, II, Advanced) – Las Vegas, NV June 24-26				
30	1	2	3	4	5	6

# September

2024

SUN	MON	TUE	WED	THU	FRI	SAT
1	2	3	4	5	6	7
	Labor Day		BOR & Committees			
8	9	10	11	12	13	14
		BOI Offsite	BOI Offsite			
	CII Fall Conference – Brooklyn, NY - September 9 – 11					
15	16	17	18	19	20	21
				Audit Committee		
22	23	24	25	26	27	28
29	30	1	2	3	4	5

# December

2024

SUN	MON	TUE	WED	THU	FRI	SAT
1	2	3	4	5	6	7
			BOR & Committees			
8	9	10	11	12	13	14
			BOI & Committees	Audit Committee		
15	16	17	18	19	20	21
22	23	24	25	26	27	28
			Christmas Day			
29	30	31	1	2	3	4



March 6, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Richard P. Bendall   
Chief Audit Executive

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Internal Audit Proposed Fiscal Year 2024-2025 Budget Request**

## RECOMMENDATION

The Audit Committee approve the Proposed Internal Audit Fiscal Year 2024-2025 Budget Request, and upon approval, direct staff to include it in LACERA's Administrative Budget for Board approval.

## BACKGROUND

According to the Institute of Internal Auditor's (IIA's) *International Standards for the Professional Practice of Internal Auditing (Standards)*, Standard 2020 the Chief Audit Executive should "communicate internal audit plans and resource requirements to senior management and the board for review and approval." In alignment with Standard 2020, the Audit Committee Charter states "the Committee is to review and approve Internal Audit's Annual Audit Plan and resource plan, to make recommendations concerning audit projects."

To remain in compliance with the above Standards and Audit Committee Charter, staff prepared the attached documents for Committee review in approving the budget request.

- **Attachment A** - Proposed Internal Audit Fiscal Year (FY) 2024-2025 Budget Request (Budget) and,
- **Attachment B** - Draft Fiscal Year 2024-2025 Internal Audit Plan

Upon Committee approval the Internal Audit Budget will be included in LACERA's Administrative Budget for Board approval.

## **BUDGET REQUEST HIGHLIGHTS**

### **Salaries and Employee Benefits (S&EB)**

The Budget Unit may make further adjustments to the S&EB numbers in our draft Budget Request. However, these adjustments would be non-discretionary increases such as cost of living adjustments and salary step increases. Internal Audit is not requesting any changes that would be subject to discretion by the Audit Committee this year, such as requests for additional positions.

### **Services and Supplies (S&S)**

Our Services and Supplies (S&S) budget request for Fiscal Year 2024-2025 remains materially unchanged from the current year's budget. The one change was to increase the amount of the budget for the Audit Committee Consultant from \$25,000 to \$50,000. Due to the depth and breadth of knowledge the new Audit Committee Consultant has in the areas of organizational ethics, compliance and risk management, staff increased the budget to leverage his knowledge as we develop our risk and compliance functions.

The most significant portion of the S&S budget is for external audit services, \$650,000. Of this, \$150,000 to \$200,000 is anticipated to be used for the external financial audit. The remaining \$400,000 will be used to perform external operational audits including IT audits, investment audits, and other consulting engagements. We plan to continue leveraging the use of our Audit Committee approved pool of external audit firms to assist us in completing our risk-based Audit Plan.

## **DRAFT FISCAL YEAR 2024-2025 INTERNAL AUDIT PLAN**

Due to the timing of the organization's budget cycle which begins early March, and Internal Audit's timeline for completing the Risk Assessment and Audit Planning process, which is completed in May, staff is providing a draft FY 2024-2025 Internal Audit Plan (Attachment B).

This year, we divided the Internal Audit Plan (Plan) into two subsections:

### **A. Enterprise Risk Management (ERM) Development Section**

We anticipate continuing to dedicate approximately twenty percent of our staffing resources to initiating a plan during Fiscal Year 2024-2025 for developing a formal ERM Program at LACERA. This is in relation to one of the key strategic goals that resulted from the recent Strategic Planning effort. Whereas the Legal Office is heading up the implementation of a formal Compliance program, Internal Audit is championing the development of a formal ERM program.

### **B. Traditional Audit Plan Section**

This section includes work on assurance, consulting and advisory, as well as Internal Audit's administrative projects planned for the upcoming Fiscal Year. We have populated the plan at this point with those projects that reoccur annually, or that we know are due to be performed, such as the financial audit and actuarial audit oversight projects. Additional projects will be added upon completion of our risk assessment/audit planning process.

Staff will complete the annual risk assessment process and provide the final Internal Audit Plan

to the Committee for approval at the June 2024 meeting. We do not anticipate that the finalization of the Plan will affect our budget. However, should that be necessary, we would prepare a budget adjustment request to accompany the Internal Audit Plan for the Audit Committee's approval for inclusion in the organization's mid-year budget request process.

### **CONCLUSION**

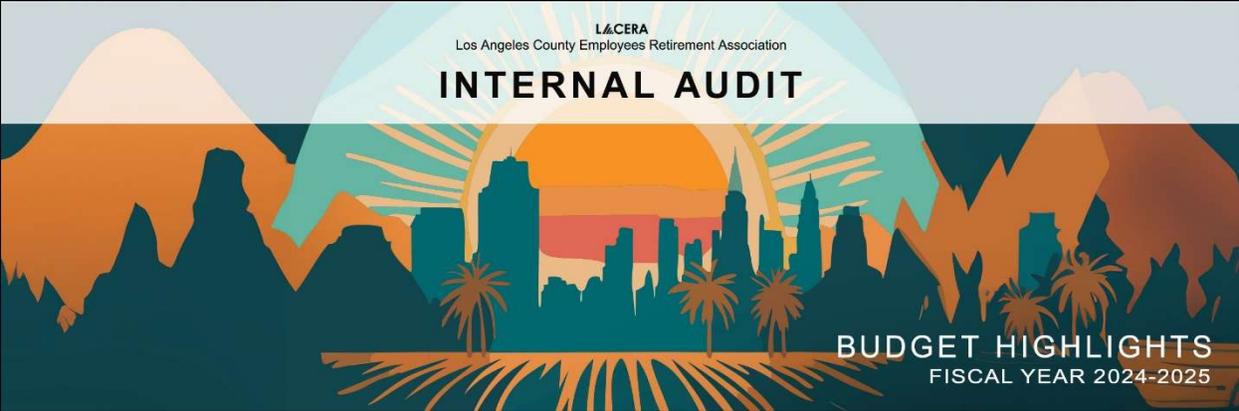
The Audit Committee approve the Proposed Internal Audit Fiscal Year 2024-2025 Budget Request, and upon approval, direct staff to include it in LACERA's Administrative Budget for Board approval.

### **Attachments:**

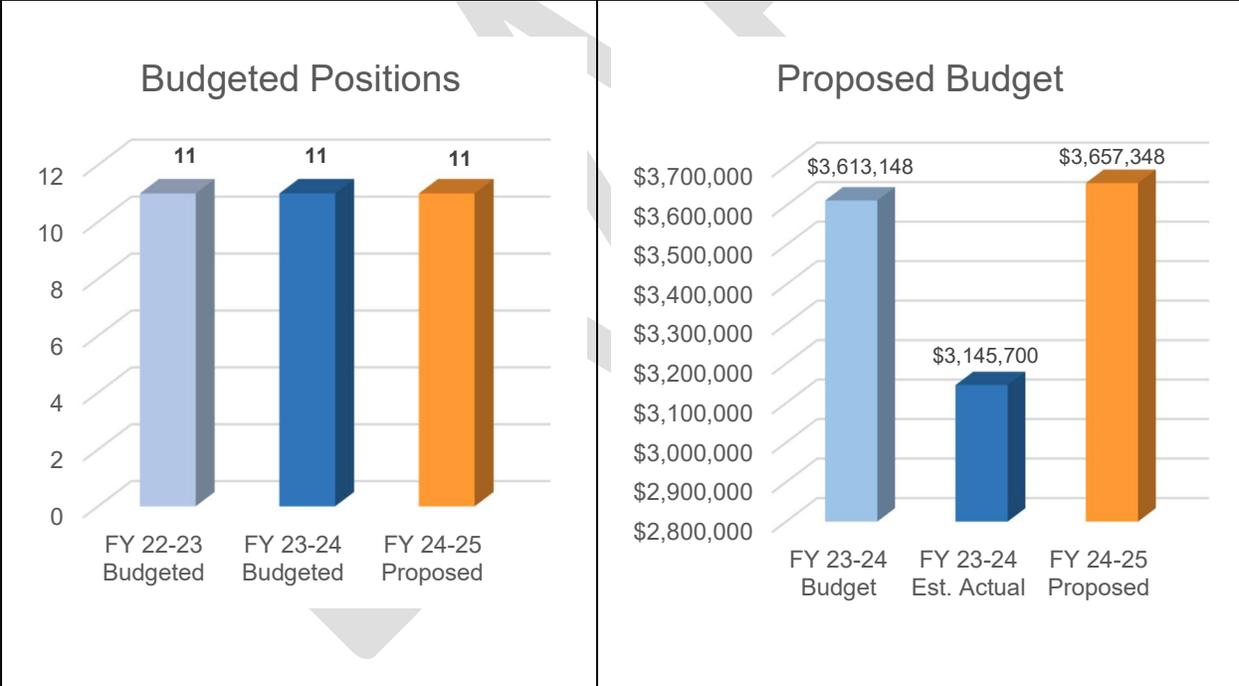
- A. Proposed FY 2024-2025 Internal Audit Budget Request
- B. Draft FY 2024-2025 Internal Audit Plan



# INTERNAL AUDIT BUDGET



The Internal Audit (IA) Division enhances and protects LACERA's values by providing independent risk-based and objective assurance, consulting, and advisory services designed to add value and improve LACERA's operations. 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. Work is performed in conformance with the Institute of Internal Auditors (IIA) standards. Internal Audit communicates engagement results, findings, and recommendations regularly to the Audit Committee of the Boards.



**Summary of Significant Changes**

<u>Description</u>	<u>Position Changes</u>	<u>Amount</u>
<ul style="list-style-type: none"> <li>Increased Audit Committee Consultant Fee by \$25,000</li> </ul>		\$50,000

## **STATUS OF FY 2023-24 PROJECTS AND INITIATIVES**

Completion of the 2023-24 fiscal year Audit Plan, including the following significant engagements:

- Consulting on Records and Information (RIM)
- Consulting on Internal Controls over Financial Reporting – Cash and Treasury
- Audit of Replacement Benefit Plan (415(b))
- Audit of Procurement of Goods
- Review of One Meeting
- Consulting on Organizational Culture
- Collaborated with the Investments Office on the RFP for the actuarial consultant and auditor
- Collaborated with various stakeholders across the organization on the RFP for organizational governance software
- Obtained IIA COSO Enterprise Risk Management (ERM) Certificate for CAE and Principals

## **FY 2024-25 STRATEGIC GOALS AND OBJECTIVES**

1. **Develop Internal Audit's Strategic Plan**, which will align with LACERA's overall strategic plan
2. **Complete the FY 2024-25 Audit Plan**, which will align with LACERA's overall strategic plan
3. **Fill vacancies**, aligned with the Investing in People strategic priority. It is essential that Internal Audit's vacancies are filled so that we can address our strategic goals and objectives.
4. **Complete Training and Development requirements**, aligned with the Investing in People strategic priority, which is budgeted against our Education Expenses. Internal Audit requires each staff member to obtain 40 continuing education hours per fiscal year. Internal Audit will use the IIA's Competency Framework to assess each staff member's competencies and divisional competencies, which will determine specific training during the year.
5. **Develop the foundation for Compliance and Enterprise Risk Management (ERM)**

## **SUMMARY OF PROPOSED BUDGETARY CHANGES: SALARIES & EMPLOYEE BENEFITS (S&EB)**

### **Non-Discretionary Salary Adjustments**

The budget reflects the final six months of negotiated cost-of-living adjustments (COLAs) included in the current Memorandum of Understanding (MOU) covering the period through December 31, 2024, and approved by the Board of Retirement and Board of

Investments for all LACERA employees, as well as salary-step progression and merit pay increases for qualified and/or eligible employees and assumed commensurate increases to employee benefits. The budget does not include any changes to salaries or benefits that may be negotiated during FY 2024-25.

### **Adjustments to Permanent Staffing**

There are currently eleven budgeted full-time positions in Internal Audit. No additional staff positions are requested currently.

### **Temporary Staffing**

Internal Audit plans to fill all open budget positions. If unsuccessful by the second quarter of the fiscal year, we will consider adding a budget for temporary staffing through the mid-year budget process.

### **Overtime Needs**

Internal Audit requested 40 hours each of overtime for the Senior Administrative Assistant and Internal Auditor positions. The overtime is necessary for the timely completion of Audit Committee meeting materials.

### **Interns**

Internal Audit does not anticipate any use of interns in FY 2024-25.

### **Rehired Retirees**

Internal Audit does not anticipate any use of rehired retirees in FY 2024-25.

If there are remaining vacancies, Internal Audit will consider this option.

## **SUMMARY OF PROPOSED BUDGETARY CHANGES: SERVICES & SUPPLIES (S&S)**

### **Removal of One-Time Expenditures**

Internal Audit does not have one-time expenditures that need to be removed in the FY 2024-25.

### **Services and Supplies Adjustments**

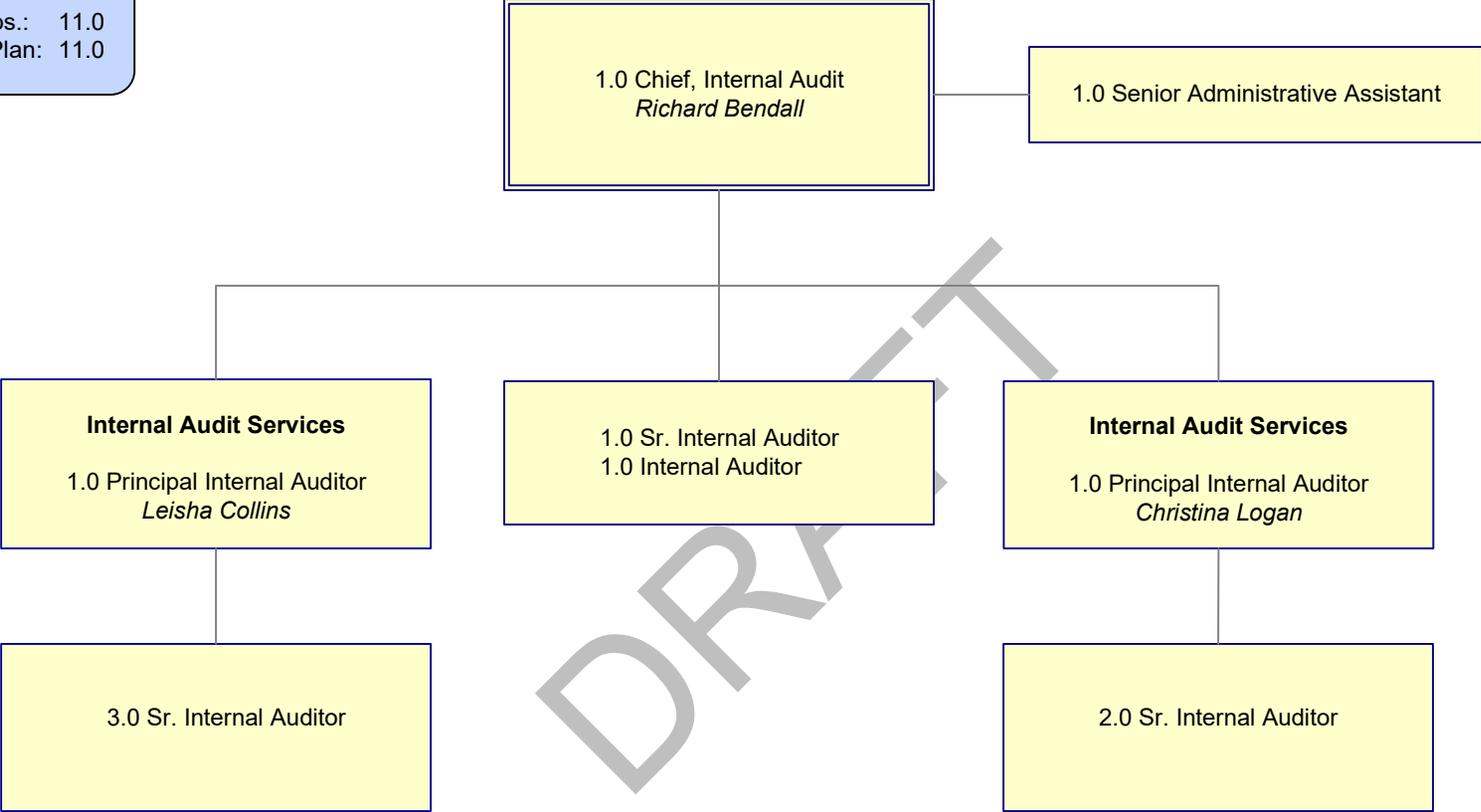
#### *Audit Committee Consultant*

Internal Audit is requesting an additional \$25,000 for the Audit Committee consultant. Staff anticipates expanding the use of the consultant based on additional expertise in compliance and enterprise risk management.

# INTERNAL AUDIT

FISCAL YEAR 2024-2025

2023-2024 Bud. Pos.: 11.0  
2023-2024 Hiring Plan: 11.0  
  
2024-2025 Bud. Pos.: 11.0  
2024-2025 Hiring Plan: 11.0



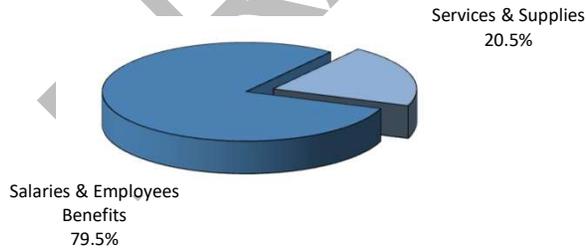
DRAFT

**LACERA**  
**FISCAL YEAR 2024-2025**  
**BUDGET SUMMARY**

**INTERNAL AUDIT**

	CURRENT YEAR 2023-2024			COMPARISON OF CURRENT YEAR BUDGET TO PROJECTION		COMPARISON OF PROPOSED BUDGET TO 2023-2024 BUDGET		
	PROPOSED BUDGET 2024-2025	YTD		OVER/(UNDER)		\$ CHANGE	% CHANGE	
		BUDGET	(01-31-24)	PROJECTION	BUDGET			% CHANGE
Salaries & Employees Benefits	\$2,908,148	\$2,888,948	\$1,260,877	\$2,425,100	(\$463,848)	-16.1%	\$19,200	0.7%
Services & Supplies	749,200	724,200	257,238	720,600	(3,600)	-0.5%	25,000	3.5%
<b>OPERATING BUDGET</b>	<b>\$3,657,348</b>	<b>\$3,613,148</b>	<b>\$1,518,115</b>	<b>\$3,145,700</b>	<b>(\$467,448)</b>	<b>-12.9%</b>	<b>\$44,200</b>	<b>1.2%</b>

**2024 - 2025 PROPOSED BUDGET**



\*All amounts rounded to the nearest dollar.

LACERA

FISCAL YEAR 2024-2025

SALARIES AND EMPLOYEE BENEFITS SUMMARY

INTERNAL AUDIT

	PROPOSED BUDGET 2024-2025	CURRENT YEAR 2023-2024			COMPARISON OF CURRENT YEAR BUDGET TO PROJECTION		COMPARISON OF PROPOSED BUDGET TO 2023-2024 BUDGET	
		BUDGET	YTD		OVER/(UNDER)		\$ CHANGE	% CHANGE
			(01-31-24)	PROJECTION	BUDGET	% CHANGE		
<b>Total LACERA Salaries</b>	<b>\$1,548,048</b>	\$1,652,147	\$772,246	\$1,444,500	(\$207,647)	-12.6%	(\$104,099)	-6.3%
<b>Total Agency Temp Salaries</b>	<b>0</b>	0	0	0	0	0.0%	0	0.0%
<b>Employee Benefits (Variable)</b>	<b>1,172,000</b>	1,065,420	416,373	832,800	(232,620)	-21.8%	106,580	10.0%
<b>Employee Benefits (Other)</b>	<b>116,500</b>	105,895	42,052	84,200	(21,695)	-20.5%	10,605	10.0%
<b>OPEB Contribution</b>	<b>64,600</b>	58,686	30,206	58,600	(86)	-0.1%	5,914	10.1%
<b>Stipends</b>	<b>0</b>	0	0	0	0	0.0%	0	0.0%
<b>Overtime</b>	<b>5,500</b>	5,300	0	5,000	(300)	-5.7%	200	3.8%
<b>Bilingual Bonus</b>	<b>0</b>	0	0	0	0	0.0%	0	0.0%
<b>Sick Leave Buyback</b>	<b>0</b>	0	0	0	0	0.0%	0	0.0%
<b>Rideshare Allowance</b>	<b>1,500</b>	1,500	0	0	(1,500)	-100.0%	0	0.0%
<b>Transportation Allowance</b>	<b>0</b>	0	0	0	0	0.0%	0	0.0%
<b>ADJUSTED GROSS S&amp;EB</b>	<b>\$2,908,148</b>	\$2,888,948	\$1,260,877	\$2,425,100	(\$463,848)	-16.1%	\$19,200	0.7%
<b>Salary Differential</b>	<b>-</b>	-	-	-	-	-	-	-
<b>TOTAL S&amp;EB</b>	<b>\$2,908,148</b>	\$2,888,948	\$1,260,877	\$2,425,100	(\$463,848)	-16.1%	\$19,200	0.7%

\*All amounts rounded to the nearest dollar.

Note: All YTD Salaries and Employee Benefits totals are as of 01/15/24, with the exception of Agency Temp Salaries, which are as of 01/31/24.

LACERA  
FISCAL YEAR 2024-2025  
SALARIES

INTERNAL AUDIT

2024-2025 BUDGET

FILLED POSITIONS		# POS.	SCHEDULE	ACTUAL MO. RATE	ANNUAL AMOUNT			
00774A	CHIEF, INTERNAL AUDIT	1	LS12	17,630	211,555			
00762A	PRINCIPAL INTERNAL AUDITOR	2	118J	27,490	329,876			
00763A	SENIOR INTERNAL AUDITOR	4	112F	46,067	552,800			
00439A	SENIOR ADMINISTRATIVE ASSISTANT	1	94B	7,046	84,547			
POSITIONS		8			1,178,778			
VACANT POSITIONS		# POS.	SCHEDULE	1ST STEP MO. RATE	ANNUAL AMOUNT	FILLED AT 12 MONTHS	FILLED AT 9 MONTHS	FILLED AT 6 MONTHS
00763A	SENIOR INTERNAL AUDITOR	2	112F	8,840	106,081	212,162		
00764A	INTERNAL AUDITOR	1	106C	7,457	89,485	89,485		
POSITIONS		3			301,647	301,647	0	0
TOTAL POSITIONS		11						
GROSS SALARIES					1,480,425			
ANTICIPATED MOU SALARY INCREASE**					0			
ANTICIPATED STEP AND/OR MERIT SALARY INCREASE					6,347			
BONUS					61,277			
120-DAY RETIREE(S)					0			
TOTAL SALARIES					1,548,048			

MAPP Tier I and Tier II positions are shown at actual salaries as of 01/01/24.  
 Represented/Non-Represented positions are shown at actual salaries as of 01/01/24.  
 Represented positions shown in blue.

Vacancies are shown at the 1st Step.

\*All amounts rounded to the nearest dollar.

\*\* Gross salaries are multiplied by 0% to calculate anticipated MOU increase.

LACERA

FISCAL YEAR 2024-2025

SERVICES & SUPPLIES ACCOUNT SUMMARY

INTERNAL AUDIT

ACCOUNT CLASSIFICATION	PROPOSED BUDGET 2024-2025	CURRENT YEAR 2023-2024			COMPARISON OF CURRENT YEAR BUDGET TO PROJECTION		COMPARISON OF PROPOSED BUDGET TO 2023-2024 BUDGET	
		BUDGET	YTD		OVER/(UNDER)		\$ CHANGE	% CHANGE
			(01-31-24)	PROJECTION	BUDGET	% CHANGE		
TRANSPORTATION & TRAVEL	\$17,000	\$17,000	\$6,297	\$14,800	(\$2,200)	-12.9%	\$0	0.0%
OFFICE SUPPLIES & EQUIPMENT	1,200	1,200	129	800	(400)	-33.3%	0	0.0%
PROFESSIONAL & SPEC. SRVCS.	700,000	675,000	239,528	675,000	0	0.0%	25,000	3.7%
EDUCATIONAL EXPENSES	30,500	30,500	11,284	29,500	(1,000)	-3.3%	0	0.0%
MISCELLANEOUS	500	500	0	500	0	0.0%	0	0.0%
TOTAL	\$749,200	\$724,200	\$257,238	\$720,600	(\$3,600)	-0.5%	\$25,000	3.5%

\*All amounts rounded to the nearest dollar.

**ATTACHMENT B**

A draft FYE 2025 Audit Plan is provided below. In accordance with our Charter, Internal Audit will use a risk based Audit Plan for the work to be performed by Internal Audit. The Final Audit Plan will be developed upon completion of our annual risk assessment and audit planning process. As illustrated below, based on past experience, we anticipate Internal Audit will devote 20 percent of available time and resources to the Enterprise Risk Management Strategic Planning effort, with 80 percent dedicated to our traditional audit plan work. Making up the 80 percent will be 20 percent focused on the Executive/Legal and Organizational level, 15 percent in each of the four remaining areas of the audit plan for a total of 100 percent. These percentages may change based on our risk assessment and audit planning process. The final plan will be presented to the Audit Committee for approval at the June meeting.

<b>DRAFT FY 2024-2025 INTERNAL AUDIT PLAN</b>			
<b>ENTERPRISE RISK MANAGEMENT (ERM) PLAN</b>			<b>20 percent</b>
<b>AUDIT PLAN</b>			
<b>AUDIT PLAN</b>			<b>80 Percent</b>
	<b>DIVISION</b>	<b>AUDIT/PROJECT NAME</b>	<b>PROJECT TYPE</b>
<b>EXECUTIVE/LEGAL/ORGANIZATIONAL</b>			<b>20 percent</b>
1	Org	LA County Rehired Retirees	Audit
2	Org	Risk Assessment	Audit
3	Org	Continuous Audit Processes (CAP)	Audit
4	Org	Reco Follow Up	Continuous
5	Exec, Legal, Org	TBD - 2 to 4 based on Risk Assessment	TBD
<b>ADMINISTRATION - Admin Services, HR Systems</b>			<b>15 percent</b>
6	HR	LACERA Rehired Retirees	Audit
7	Systems	Oversight of SOC Audits FY 24 & 25	Oversight
8	Admin, HR, Systems	TBD - 2 to 4 based on Risk Assessment	TBD
<b>INVESTMENTS &amp; FASD</b>			<b>15 Percent</b>
8	FASD	CEO Credit Card	Audit
9	FASD	Oversight of Financial Audit FY 24 & 25	Oversight
10	Investments	Oversight of Actuarial Audit FY 24 & 25	Oversight
11	Investments	Oversight THC Financial Audits - FY 24 & 25	Oversight
12	Investments/FASD	TBD - 2 to 4 based on Risk Assessment	TBD
<b>OPERATIONS - Benefits, DRS, RHC, Member Services</b>			<b>15 Percent</b>
13	Various	TBD - 2 to 4 based on Risk Assessment	TBD
<b>INTERNAL AUDIT OPERATIONS</b>			<b>15 percent</b>
14	Internal Audit	Professional Development / CPE	Other Projects
15	Internal Audit	QAIP	Other Projects
16	Internal Audit	AC Support	Other Projects
17	Internal Audit	TeamMate	Other Projects



March 5, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Nathan K. Amick   
Senior Internal Auditor

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Bank of America Wire Transfer Audit**

### **RECOMMENDATION**

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

1. Accept and file report,
2. Instruct staff to forward report to Boards or Committees,
3. Make recommendations to the Boards or Committees regarding actions as may be required based on audit findings, and/or
4. Provide further instruction to staff.

### **ENGAGEMENT REPORT**

Bank of America Wire Transfer Audit  
(Report Issued: March 5, 2024)

Noted and Reviewed:



Richard P. Bendall  
Chief Audit Executive

NKA



**LACERA INTERNAL AUDIT DIVISION**

**Bank Of America Wire Transfer Audit**

**March 5, 2024**

**AUDIT PERFORMED BY:**

**Nathan K. Amick**  
Senior Internal Auditor

## AUDIT REPORT

<b>Audit Name:</b>	Bank of America Wire Transfer Audit
<b>Responsible Division:</b>	Investments Office and Financial Accounting Services Division (FASD)
<b>Audit Rating*:</b>	Satisfactory
<b>Prior Audit Rating*:</b>	N/A
<b>Prior Report Date:</b>	October 2, 2018

### BACKGROUND

As part of the Fiscal Year Ending 2024 Audit Plan, we examined LACERA's Bank of America CashPro (CashPro) wire transfer process. We perform wire transfer audits on a fairly regular cyclical basis (every two to three years) due the inherent risks associated with wiring large sums of money. This audit follows our audit of LACERA's custodial bank, State Street Bank's wire transfer system, for which Internal Audit issued a "Satisfactory" report in June 2023.

Before October 2022, the CashPro system was used more extensively by LACERA's Investment Office and FASD for all wire transfers related to the real estate portfolio. This included wire transfers to Advisors to fund acquisitions of properties, for the payment of vendors, to receive distributions related to the properties from the Advisors, and also for the internal transfer between property accounts.

As of October 2022, the use of CashPro by the Investments Office and FASD was reduced significantly. In an effort to reduce operational risk, and in accordance with the Investments Office's Real Assets and Inflation Hedges 2021 Structure Review, LACERA leveraged the Advisor's cash management capabilities and transitioned wire roles and responsibilities in their entirety to the Advisors. Currently, the Investments Office and FASD are only executing wires related to LACERA's headquarter building (Gateway Plaza), which the Investments Office manages internally. The CashPro process is only used by Investments/FASD for two key functions:

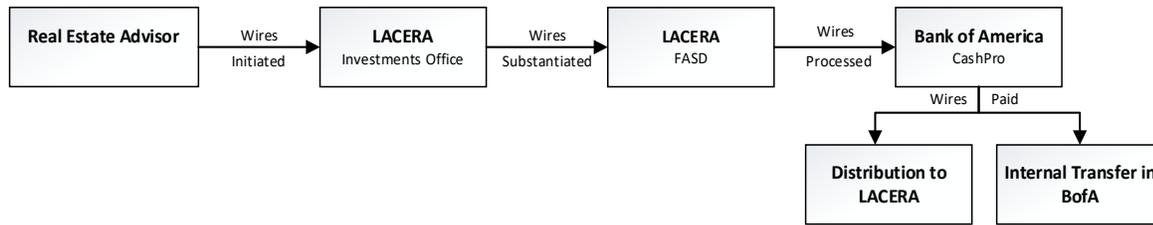
1. Receipt of revenue distributions from Gateway Plaza
2. Internal transfers between Gateway Plaza accounts

As Investments and FASD have no involvement or control over the use of the CashPro system by the Advisors, this audit was very limited in scope only to wires related to Gateway Plaza.

Wires for Gateway Plaza are initiated once the property manager sends notification to LACERA's Investments Office Real Estate Team (Real Estate Team) which include the relevant wire details. The Real Estate Team thoroughly examines the request and then forwards it to FASD staff for further processing and FASD management approval. Once approved by FASD Management, FASD staff enters the wire instructions into CashPro and executes the wire. CashPro incorporates built-in segregations of duties. This means that one person is responsible for entering the data, while another person approves the data and releases the wire, as illustrated below:

---

\* See Appendix 1 for Audit Rating



During the period from October 2022 to December 2023, LACERA facilitated a total of 18 wire transactions for its property located at 300 N Lake Avenue. These transactions comprised five distributions and thirteen transfers, amounting to a sum of \$17.3 million.

### **AUDIT OBJECTIVE & SCOPE**

Based on Internal Audit's risk assessment, this engagement was focused on evaluating the adequacy of controls around the CashPro wire transfer process for:

- Effectiveness of Operations and Controls – Assess whether security controls for wires processed through CashPro system have been designed to produce the desired or intended results, and controls to mitigate risk are adequate and operating effectively.
- Compliance with Applicable Policies, Laws and Regulations: - Assess the controls over LACERA's operations to determine whether wires were documented, authorized, and processed accurately.

The audit scope period for this audit was October 1, 2022, to December 31, 2023. This audit was performed in accordance with the Institute of Internal Auditors' International (IIA) Standards for the Professional Practice of Internal Auditing

### **AUDIT RATING & SUMMARY OF FINDINGS**

In our opinion, the effectiveness of controls applicable to the audit scope are **Satisfactory**. Investments and FASD have adequate controls over the CashPro and wire process as it relates to opening of new accounts, user access and authorization, administrator rights, segregation of duties, and the authorization, accuracy, and completeness of wire transactions. Based on our testing performed, we have no audit findings to report. The table below provides a summary of audit objectives, associated controls tested and the results.

<b>Audit Results Dashboard – Bank Of America CashPro Wire Transfer Process</b>		
<b>Audit Objective(s)</b>	<b>Associated Control Attributes</b>	<b>Test Results</b>
Effectiveness of Operations and Controls	Opening of new bank accounts are performed by appropriate and authorized personnel	No exceptions noted
Effectiveness of Operations and Controls	Access to CashPro application is limited to authorized personnel	No exceptions noted
Effectiveness of Operations and Controls	CashPro Administrators cannot modify their own access rights	No exceptions noted
Effectiveness of Operations and Controls	CashPro requires segregation of duties for all wires	No exceptions noted
Compliance to Applicable Policies, Laws, and Regulations	Wire transfers are appropriate, authorized and supported by source documentation	No exceptions noted
Compliance to Applicable Policies, Laws, and Regulations	Wire transfers are properly reconciled and recorded	No exceptions noted

We would like to thank both the FASD and Investments Division staff for their cooperation with this audit.

**REVIEWED AND APPROVED**



Richard P. Bendall  
Chief Audit Executive

**Date:** March 5, 2024

**REPORT DISTRIBUTION**

2024 Audit Committee	Santos H. Kreimann, CEO	Stephen Rice, Chief Legal Counsel
2024 Plante Moran Audit Team	Luis Lug, DCEO	Ted Granger, CFO
Larry Jensen, Audit Committee Consultant	Laura Guglielmo, AEO	Jonathan Grabel, CIO
	JJ Popowich, AEO	

## **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.



# Bank of America Wire Transfer Audit

**Audit Report Date:** March 5, 2024

---

Presented by:

Nathan K. Amick, Senior Internal Auditor

# Summary of Engagement



Responsible Division:	Investments Division and the Financial & Accounting Services Division
Type of Engagement:	Assurance
Audit Rating:	Satisfactory

## **Type of Engagements**

**Assurance:** 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.

**Consulting:** Collaborate with Management to provide a formal assessment and advice for improving LACERA's governance, risk management, and control processes, without Internal Audit assuming Management responsibility.

**Advisory:** Provide Management with informal advice.

# Background, Objective, Scope



## **Background**

Investments Division and FASD use the Bank of America CashPro systems to execute wires transfers related to LACERA's real estate portfolio. During the period from October 2022 to December 2023, LACERA facilitated a total of 18 wire transactions totaling \$17.3 million.

## **Objective**

Evaluate the adequacy of controls around the CashPro wire transfer process for:

- Effectiveness of Operations and Controls – Assess whether security controls for wires processed through CashPro system have been designed to produce the desired or intended results, and controls to mitigate risk are adequate and operating effectively.
- Compliance with Applicable Policies, Laws and Regulations: - Assess the controls over LACERA's operations to determine whether wires were documented, authorized, and processed accurately.

## **Scope**

Engagement scope included 100% of CashPro wires processed by Investments/FASD for the period of October 1, 2022 to December 30, 2023.

# Engagement Results



We gave this audit a “Satisfactory” rating. We identified no reportable conditions and have no recommended areas for improvement. Below is a summary of the testing performed.

CONTROL OBJECTIVES	TEST RESULTS
Opening of new bank accounts are performed by appropriate and authorized personnel	No exceptions noted
Access to CashPro application is limited to authorized personnel	No exceptions noted
CashPro Administrators cannot modify their own access rights	No exceptions noted
CashPro requires segregation of duties for all wires	No exceptions noted
Wires transfers are appropriate, authorized and supported by source documentation	No exceptions noted
Wire transfers are properly reconciled and recorded	No exceptions noted

# Questions





March 6, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Gabriel Tafoya   
Senior Internal Auditor

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Procurement of Goods Audit**

### **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,
2. Instruct staff to forward report to Boards or Committees,
3. Make recommendations to the Boards or Committees regarding actions as may be required based on audit findings, and/or
4. Provide further instruction to staff.

### **ENGAGEMENT REPORT**

Procurement of Goods Audit  
(Report Issued: March 6, 2024)

Noted and Reviewed:



Richard P. Bendall  
Chief Audit Executive

GT



**LACERA INTERNAL AUDIT DIVISION**

**Procurement of Goods Audit**

**March 6, 2024**

**AUDIT PERFORMED BY:**

**Gabriel Tafoya, CISA**  
Senior Internal Auditor

## AUDIT REPORT

<b>Audit Name:</b>	Procurement of Goods Audit
<b>Responsible Division:</b>	Administrative Services Division
<b>Audit Rating*:</b>	Opportunities for Improvement
<b>Prior Audit Rating*:</b>	N/A
<b>Prior Report Date:</b>	N/A

### **BACKGROUND**

We reviewed LACERA's Procurement of Goods Process as part of Internal Audit's Fiscal Year End (FYE) 2023-2024 Audit Plan. The overall objective of the audit was to assess if controls are designed adequately and operating effectively in compliance with the Policy for Purchasing Goods and Services (Policy) and the Purchasing and Contracting Administration Manual (Manual).

LACERA employs a centralized procurement unit within the Administrative Services Division that is charged with acquiring and purchasing goods and equipment for the organization. The Procurement Unit ensures:

- Procurements are compliant with the Policy.
- Purchases are made from authorized vendors at the appropriate prices or terms.
- Individuals ordering and receiving goods/supplies are authorized to do so.
- Purchase orders are complete and accurate.
- Purchases are properly reviewed and approved prior to being processed.

Buyers are authorized purchasing agents of the Procurement Unit. Buyers are aligned with specific departments, which improves the overall control environment, quality client services, and procurement cycle time. Buyers perform all necessary acquisition steps, including:

- Bidding and price negotiation
- Placing orders for goods
- Purchase order processing
- Receipt of purchased goods

LACERA's procurement expenditures totaled approximately \$5.2 million, across 15 divisions for FYE 2023 and there was a total of 479 invoice payment transactions for the period. This audit covers procurement of goods and does not include contract operations and services, which were audited in 2022.

---

\* See Appendix 1 for Audit Rating

**AUDIT OBJECTIVES AND SCOPE**

Based on Internal Audit’s engagement risk assessment, we focused this engagement on program compliance with the Procurement Policy and Manual. The objectives for this audit were to assess:

- Effectiveness of Operations and Controls – Assess whether procurement processes have been designed to produce the desired or intended results and controls to mitigate risk.
- Compliance with Applicable Policies, Laws and Regulations: - Assess whether procurement purchases and activities have been carried out in accordance with applicable policies and procedures as stated in the Procurement Policy and Manual:

The engagement scope included review of procurement transactions occurring between July 1, 2022 - June 30, 2023. The audit was performed in accordance with the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing.

**AUDIT RATING & SUMMARY OF FINDINGS**

Overall, the Procurement Unit has adequate controls relating to the oversight of the procurement process. Internal controls were generally efficient and effective; however, we did identify opportunities for improvements in some areas as noted below. We have rated this audit in the category of **Opportunities for Improvement**. The Audit Results Dashboard shows each process reviewed, the associated control attributes tested, and the test results leading to the audit findings.

Audit Results Dashboard – Procurement of Goods Audit		
Audit Objectives	Associated Control Attributes Tested	Test Results
Assess effectiveness of Operations and Internal Controls	Procurement policies and procedures are formally documented, approved, and provided to key stakeholders	No Exceptions
	Policies and procedures are reviewed and updated frequently, and training provided	Finding #1
	Multi-level approval process is in place with defined and segregated roles and responsibilities.	No Exception
	Separation of requisition, buyer, and receipt of good responsibilities	No Exception
	There are defined spending limits and approval requirements	No Exceptions
	Criteria has been established requiring the use of a 3-bid process at specified dollar thresholds.	No Exceptions
	A three-way match is required comparing pertinent data between the purchase order, invoice, and receiving document	No Exceptions
	Procurement requires and maintains documentation supporting purchases.	No Exceptions

<b>Audit Results Dashboard – Procurement of Goods Audit (Cont.)</b>		
<b>Audit Objectives</b>	<b>Associated Control Attributes Tested</b>	<b>Test Results</b>
Compliance with applicable, policies procedures	Purchases are only made by individuals on the list of Authorized Divisional Requesters (ADRs).	No Exceptions
	Purchases are supported with required documentation and are properly reviewed and approved.	Finding #2
	The process of matching items received to items requested and invoiced is conducted and clearly documented.	Finding #3
	FASD receives copies of the purchase orders, and corresponding packing slip and invoice to confirm goods requested, match goods received, and invoiced before initiating payment.	No Exceptions
	The justification for the use of sole and single source approvals are clearly documented and supported with appropriate levels of approval	Finding #4
	The exclusion of the lowest bid, in a 3-bid process, is clearly and sufficiently documented and approved.	Finding #5
	Purchases and distribution of organizational forms is adequately tracked.	Finding #6

A total of six (6) audit findings were issued related to operational controls. Each of the below Findings are detailed in the subsequent pages, including our Recommendations and Management Responses.

**Summary of Findings**

<b>Finding#</b>	<b>Page</b>	<b>Finding Title</b>	<b>Risk Rating**</b>
F1	5	The Procurement Policy and Manual are outdated.	Medium
F2	7	Missing and incomplete procurement forms and supporting documentation.	Medium
F3	9	Missing documentation of the verification of receipt of goods.	Medium
F4	10	Missing and unclear documentation supporting justification for use of Single and Sole Source Vendors.	Medium
F5	12	Insufficient documentation for excluding the lowest bidder in a three-bid process.	Medium
F6	13	Inefficiencies and discrepancies noted on the Inventory Tracking Spreadsheets.	Low

\*\*See Appendix 2 for Findings' Risk Rating

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

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

**REVIEWED AND APPROVED**



Richard P. Bendall  
Chief Audit Executive

**Date:** March 6, 2024

**REPORT DISTRIBUTION**

2024 Audit Committee	Santos H. Kreimann, CEO	J.J. Popowich, AEO
2024 Plante Moran Audit Team	Luis Lugo, DCEO	Ricki Contreras, Manager, Administrative Services
Larry Jensen, Audit Committee Consultant	Laura Guglielmo, AEO	Internal Audit Group

## **FINDING #1**

**The Procurement Policy and Manual are outdated.**

**Risk Level\*\***  
Medium

### **OBSERVATION**

The Policy for Purchasing Goods and Services (Policy) and the Purchasing and Contracting Administration Manual (Manual) provides guidance for the procurement of goods and the selection of service providers for LACERA. Both the Policy and Manual applies to all Contract Administrators and purchasing agents who participate in the procurement of goods and services.

As part of our audit, we reviewed the Policy and Manual and compared it to current practices. We noted that the Manual indicates it should be updated annually but was last updated in February 2020, and the Policy should be updated biennially and was last updated in November 2019. Furthermore, Internal Audit previously recommended the updating of the Policy in the 2023 Contract Operations Audit with a 12/31/2023 target date for implementation.

In comparison with current practices some examples we noted for updates include (but are not limited to) the following:

1. Use of adobe e-signature for approvals in lieu of wet signature, and or email approvals.
2. Clarification of requirements for the receipt of goods and documentation confirming three-way match.
3. More detailed information, guidance regarding the criteria and use of sole and single source vendors.
4. Relevant procedures that address the process for ordering and tracking forms and publications for the Communications Division and other divisions.

Policies and procedures provide guidance in the pursuit of achieving the objectives of the process. They also help reduce misunderstandings and increase distribution of pertinent information to those involved in the process. As an integral component of the governance surrounding LACERA's procurement process, the Policy and Manual should undergo more frequent reviews and updates. Periodic training should also be provided.

### **RISK**

Outdated or incomplete policies and procedures increase the risk of non-compliance, including the risk of improper or unauthorized purchases.

### **RECOMMENDATIONS**

1. Administrative Services Management should update the Policy for Purchasing Goods and Services (Policy) and the Purchasing and Contracting Administration Manual in accordance with the Policy's requirement.
2. Administrative Services Management should provide training on the updated Policy and Manual to reinforce adherence.

---

\*\* See Appendix 2 for Findings' Risk Rating

### **MANAGEMENT RESPONSE**

---

Management agrees with Finding #1 of the Procurement of Goods Audit. The Policy was revised and is under review by the new Administrative Services Manager who was recently transferred to the division in December 2023, which delayed its implementation. The updated Policy and Manual are undergoing further revision to incorporate new workflows consistent with the recently implemented Electronic Contract Lifecycle Management (ECLM) system and a newly proposed centralized vendor management program. Final revisions, implementation and associated training will be completed by 06/30/2024.

### **TARGET COMPLETION DATE**

---

**6/30/2024**

## **FINDING #2**

**Missing and incomplete procurement forms and supporting documentation.**

**Risk Level\*\***  
Medium

### **OBSERVATION**

Our audit work included testing of purchases to assess compliance with the Procurement Policy and Manual. According to Section III of the Manual - *Procedures for Purchasing Equipment and Other Goods*, “In order to purchase a special supply item, the requestor must complete a Special Supply Request form to the Procurement Unit with the following information”:

- a. Requisition Date
- b. Requestors name and phone extension
- c. Organization code and GL account number
- d. Preferred vendor, if any
- e. Name of item
- f. Catalogue page/item number, if known
- g. Product description or estimated cost, if known
- h. Brief justification for the purchase (include need/benefit to staff, etc.)

In addition, Section 8 – Centralized Purchasing, “Buyers and Contract Administrators must document all transactions according to established procurement procedures and maintain such documentation for audit purposes”.

From a sample of forty-one (41) Procurement Packet transactions tested, we noted the following issues of non-compliance:

- Twenty-three (23) were missing information on the Special supply Request (SSR), for example, order received by signature and received by date missing, the grand total and estimated cost are missing, and the SSR is missing from the PO-Packet.
- One instance where the sequence of the supporting documentation was out of sequence; invoice or PO date was prior to the SSR.
- Three (3) missing the SSR.
- One (1) was missing on-line Amazon detail information for the order.
- One (1) was missing the packing slip.
- One (1) was missing the Receiving Posting Journal and the Receiving Distribution Detail reports.
- One (1) License Agreement form was missing the Witness Signature and Date.
- One (1) was missing the SSR, Contract Agreement, and Vendor Quote Summary.

While individually these exceptions may appear as minor infractions with low-level risk, collectively they indicate a fractured process and a lack of adherence to controls by staff. Overall, this underscores the need for more frequent training to reinforce procurement guidelines and requirements.

---

\*\* See Appendix 2 for Findings' Risk Rating

### **Risk**

---

Noncompliance with established procedures and inadequate oversight could increase the risk of fraud, loss, or undetected error.

### **RECOMMENDATION**

---

3. Administrative Services Management should provide training to staff once the Policy and Manual are updated to ensure that staff are aware of requirements for the procurement and receipt of goods.

### **MANAGEMENT RESPONSE**

---

Management agrees with Finding #2 of the Procurement of Goods Audit. As indicated in Finding #1 the updated Policy and Manual will be finalized, implemented, and associated training will be completed by 06/30/2024.

### **TARGET COMPLETION DATE**

---

**6/30/2024**

### **FINDING #3**

**Missing documentation of the verification of receipt of goods.**

**Risk Level\*\***  
Medium

### **OBSERVATION**

The Procurement process includes two key controls to ensure that items received match items requested and invoiced: 1) upon receipt of goods, the Procurement Unit delivers the items to the requestor who matches the goods received to good requested on the Special Supply Request (SSR) and then signs the SSR indicating receipt and 2) the Procurement Unit performs a 3-way match that compares: the purchase order (PO), the order receipt or packing slip, and the invoice. The goal of these controls is to identify any discrepancies and to validate the accuracy of invoices before Financial Accounting Services Division (FASD) proceeds with processing invoice payment.

Based on our testing of the forty-one (41) procurement purchases we noted:

- Ten (10) instances where the SSRs did not include the receiving divisions signature of receipt.
- Thirty-four (34) were missing documented evidence that a three-way match was performed.

Although we noted there was a lack of completed documentation and missing evidence of the 3-way match, we confirmed that each purchase matched the items and dollar amounts on the PO and invoice. However, it's important that staff perform these steps as part of the procurement process to identify errors prior to the initiation of vendor payments.

### **RISK**

The absence of adherence to the above controls increases the risk of overlooking errors and paying for items that have not been received.

### **RECOMMENDATION**

4. Procurement Management ensure that the three-way match between the PO, Invoice, and packing slip is performed and documented. This criterion should be included in the Policy and Manual, and training provided to staff.

### **MANAGEMENT RESPONSE**

Management agrees with Finding #3 of the Procurement of Goods Audit. The three-way match procedure is now executed in Certify AP (the new automated accounts payable system). All staff have been trained as of January 25, 2024.

### **TARGET COMPLETION DATE**

**COMPLETED**

\*\* See Appendix 2 for Findings' Risk Rating

## **FINDING #4**

---

**Missing and unclear documentation supporting justification for use of Single and Sole Source Vendors.**

**Risk Level\*\***  
Medium

## **OBSERVATION**

In accordance with the Policy, a sole-source procurement (sole source) is one in which only one vendor can supply the commodity or service. This may occur when the goods or services are specialized or unique in character. Sole source means the vendor is “the one and only” seller of the product. A single-source procurement (single source) is one in which, although two or more vendors supply the commodity or service, a specific vendor is selected for substantial and justified business benefits/purposes, thereby eliminating the competitive bidding process.

According to section II of the Policy, a written justification must be provided to the Purchasing Agent when a sole source or single source procurement is required. Furthermore, the Policy states the written justification should include:

- Explanation of why a unique Scope of Work for a Good or Service is required;
- Details on the unique features of the Good or Service;
- Reason that competing vendor’s Goods or Services are not satisfactory;
- Any other relevant information to support the sole/single-source documentation.

The Policy also includes an example of the Justification Letter with the required documentation which states that, when using a Single Source Vendor, the written justification should include a statement of actions to be taken to preclude the necessity of using a single source vendor in the future.

We performed detailed testing of twenty-three (23) transactions that included the use of single or sole source vendors. Our testing disclosed the following exceptions relating to the Single or Sole Source Justification Letter:

- Nine (9) instances where justification was not clearly stated or was missing entirely.
- Twenty-one (21) instances where the description of the future actions that will be taken to prevent future use of single source acquisition of the same supplies/services was missing.
- Five (5) missing division manager approvals; four (4) of them were signed by the Assistant Manager, and one (1) signed by the Communications Creative Coordinator.
- We also noted that the Policy is ambiguous as to the use of the single and sole source vendors resulting in the following inconsistencies or deficiencies:
  - Several instances where both terms were used interchangeably within a Justification Letter.
  - The use of the term single source, with a description relating to sole source,

---

\*\* See Appendix 2 for Findings’ Risk Rating

- Instances where the justifications did not clearly convey the business reason/justification for using a single or sole source vendor.
- Use of the same single source vendors for several years, without going out to bid to assess competitive pricing.
- No documentation supporting that the Procurement buyer had made a determination of the reasonableness of the price for the product.

Overall, we noted that there does not appear to be clear criteria and controls around the practice of using sole and single sourced vendors. This is necessary to ensure LACERA is compliant with fair and open competitive procurement practices, obtaining best value and quality, while allowing for the use of sole and single source vendors with appropriate business justification.

### **RISK**

Demonstrating open and fair procurement practices, in compliance with LACERA's Procurement Policy, could be brought into question if the integrity of the use of single and sole source is not maintained, clearly defined, and documented.

### **RECOMMENDATIONS**

5. Administrative Services management should evaluate the pervasive use of single and sole source vendors and clarify the criteria and supporting documentation necessary to justify the practice.
6. Procurement Supervisors should ensure that requesters and procurement staff comply with providing the appropriate documentation and justification to support sole and single source procurements.

### **MANAGEMENT RESPONSE**

Management agrees with Finding #4 of the Procurement of Goods Audit. The revised Policy and Manual will clearly outline criteria and the required supporting documentation to support the use of single and sole source vendors. This Policy will be in place by 6/30/2024 and effective 07/01/2024, Administrative Services will have direct oversight of LACERA's centralized vendor management program. This team will ensure compliance will all solicitation requirements.

### **TARGET COMPLETION DATE**

**6/30/2024**

## **FINDING #5**

**Insufficient documentation for excluding the lowest bidder in a three-bid process.**

**Risk Level\*\***  
Medium

## **OBSERVATION**

According to section 13.1.1 B, from the Policy, procurements between \$5,001 and \$150,000 require a minimum of three (3) written bids/proposals. Activities in this category require approval by the Administrative Services Division Manager, or approved designee.

Our total sample selection for audit testing included forty-one (41) transactions and three (3) of the forty-one were transactions that went through the 3-bid process. Based on our test work we found that vendors for these three procurements were selected as required. However, we also noted a lack supporting documentation as follows:

- One (1) purchase lacked sufficient documentation to justify the selection and approval of a vendor that did not provide the lowest bid on the Vendor Quote Summary.

When using the 3-bid process, justification of the selection of a higher bid should be adequately documented to allow management sufficient information to make an informed decision of approval. Furthermore, management or designee approval should always be documented as proof that the selection was reviewed and approved by appropriate levels of management.

## **RISK**

Compliance with LACERA's Procurement Policy, demonstrating open and fair procurement practices, could be brought into question if the integrity of the 3-bid process is not maintained.

## **RECOMMENDATION**

7. Update the Policy and Manual to include guidelines for selecting a bid if the lowest one is not accepted; a detailed explanation for the reason should be documented.

## **MANAGEMENT RESPONSE**

Management agrees with Finding #5 of the Procurement of Goods Audit. The revised Policy and Manual will include guidelines for selecting a bid if the lowest is not accepted including required supporting documentation. This Policy will be in place by 6/30/2024 and effective 07/01/2024, Administrative Services will have direct oversight of LACERA's centralized vendor management program. This team will ensure compliance will all solicitation requirements.

## **TARGET COMPLETION DATE**

**6/30/2024**

\*\* See Appendix 2 for Findings' Risk Rating

## **FINDING #6**

**Inefficiencies and discrepancies noted on the Forms Inventory Tracking Spreadsheets.**

**Risk Level\*\***  
Low

### **OBSERVATION**

The procurement of forms (e.g., Plan Booklets, LACERA brochures, and member application forms) is a shared responsibility between the Communications (Communications) and the Procurement Unit. Communications is responsible for ordering forms and submits SSRs to the Procurement Unit who places the orders. The Procurement Unit is also responsible for managing the receipt and distribution of forms to LACERA's member facing divisions. The inventory is recorded on an excel spreadsheet to track the balance of forms on hand and identify when forms are depleted to thresholds requiring reordering.

Overall, we found opportunities to improve the process and for improved collaboration between the two divisions to make the process of ordering forms more efficient. Per our review, we noted some minor inefficiencies. For example, the Procurement Unit and Communication are each tracking the purchases and inventory of forms on different worksheets which increases the risk of ordering forms in an inefficient and untimely manner. In addition, the inventory worksheets need updating to include relevant information such as a record of the divisions that are requesting the form, date of form request, date of delivery, and number of forms.

Currently, Systems management is working with Procurement to develop a Forms Inventory Tracking component within the Service Now system which will be used to initiate procurement orders from start to finish as well as keep accurate inventory and tracking of Forms.

### **RISK**

Tracking of forms inventory by two separate divisions may lead to inaccuracies and inefficiencies in ordering forms.

### **RECOMMENDATION**

8. Management from Administrative Services, Communications Division and other key stakeholders involved in the process of ordering forms should discuss and collaborate on additional controls to incorporate into the updated process for purchasing and inventory of forms.

### **MANAGEMENT RESPONSE**

LACERA Management agrees with Finding #6 of the Procurement of Goods Audit. Consistent with LACERA's values of collaboration and accountability, Management expects and has directed divisions to work cooperatively to agree upon an alternative means to track the inventory of forms to be used and updated by all impacted divisions. Agreement will be reached on the shared tool to track inventory of forms and impacted divisions will begin using that new tool by 06/30/2024.

### **TARGET COMPLETION DATE**

**6/30/2024**

\*\* See Appendix 2 for Findings' 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.

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



# Procurement of Goods Audit

**Audit Report Date:** March 6, 2024

---

Presented by:  
Gabriel Tafoya, Senior Internal Auditor

# Summary of Engagement



Responsible Division:	Administrative Services Division
Type of Engagement:	Assurance
Audit Rating:	Opportunities for Improvement
Prior Audit Rating:	N/A

## Type of Engagements

**Assurance:** 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.

**Consulting:** Collaborate with Management to provide a formal assessment and advice for improving LACERA's governance, risk management, and control processes, without Internal Audit assuming Management responsibility.

**Advisory:** Provide Management with informal advice.



## **Background**

We reviewed LACERA's Procurement of Goods as part of the Fiscal Year 2023-2024 Audit Plan. LACERA maintains a Procurement Unit within the Administrative Division to facilitate the Procurement of Goods as described and permitted within its Policy for Purchasing Goods and Services (Policy).

## **Objectives**

The audit objectives were to assess program compliance with LACERA's Policy. The compliance areas reviewed for this audit include verification that:

- Procurements are compliant with the Policy.
- Purchases are made from authorized vendors at the appropriate prices or terms.
- Individuals ordering and receiving goods/supplies are authorized to do so.
- Purchase orders are complete and accurate.
- Purchases are properly reviewed and approved prior to being processed.



## **Scope**

The engagement scope included review of procurement transactions occurring between July 1, 2022 - June 30, 2023.

# Audit Results



Audit Results Dashboard – Procurement of Goods Audit		
Audit Objectives	Associated Control Attributes Tested	Test Results
Assess effectiveness of Operations and Internal Controls	Procurement policies and procedures are formally documented, approved, and provided to key stakeholders	No Exceptions
	Policies and procedures are reviewed and updated frequently, and training provided	Finding #1
	Multi-level approval process is in place with defined and segregated roles and responsibilities.	No Exception
	Separation of requisition, buyer, and receipt of good responsibilities	No Exception
	There are defined spending limits and approval requirements	No Exceptions
	Criteria has been established requiring the use of a 3-bid process at specified dollar thresholds.	No Exceptions
	A three-way match is required comparing pertinent data between the purchase order, invoice, and receiving document	No Exceptions
	Procurement requires and maintains documentation supporting purchases.	No Exceptions

# Audit Results



<b>Audit Results Dashboard – Procurement of Goods Audit</b>		
<b>Audit Objectives</b>	<b>Associated Control Attributes Tested</b>	<b>Test Results</b>
Compliance with applicable, policies procedures	Purchases are only made by individuals on the list of Authorized Divisional Requesters (ADRs).	No Exceptions
	Purchases are supported with required documentation and are properly reviewed and approved.	Finding #2
	The process of matching items received to items requested and invoiced is conducted and clearly documented.	Finding #3
	FASD receives copies of the purchase orders, and corresponding packing slip and invoice to confirm goods requested, match goods received, and invoiced before initiating payment.	No Exceptions
	The justification for the use of sole and single source approvals are clearly documented and supported with appropriate levels of approval	Finding #4
	The exclusion of the lowest bid, in a 3-bid process, is clearly and sufficiently documented and approved.	Finding #5
	Purchases and distribution of organizational forms is adequately tracked.	Finding #6

# Summary of Findings



Finding #	Title of Finding	Rating	Management Response
1	The Procurement Policy and Manual are outdated.	Medium	<p>Agree. Administrative Services will:</p> <ul style="list-style-type: none"> <li>Management agrees with Finding #1 of the Procurement of Goods Audit. The Policy was revised and is under review by the new Administrative Services Manager who was recently transferred to the division in December 2023, which delayed its implementation. The updated Policy and Manual are undergoing further revision to incorporate new workflows consistent with the recently implemented Electronic Contract Lifecycle Management (ECLM) system and a newly proposed centralized vendor management program. Final revisions, implementation and associated training will be completed by 06/30/2024.</li> </ul>
2	Missing and incomplete procurement forms and supporting documentation.	Medium	<p>Agree. Administrative Services will:</p> <ul style="list-style-type: none"> <li>Management agrees with Finding #2 of the Procurement of Goods Audit. As indicated in Finding #1 the updated Policy and Manual will be finalized, implemented, and associated training will be completed by 06/30/2024.</li> </ul>
3	Missing documentation of the verification of receipt of goods.	Medium	<p>Agree. Administrative Services will:</p> <ul style="list-style-type: none"> <li>Management agrees with Finding #3 of the Procurement of Goods Audit. The three-way match procedure is now executed in Certify AP (the new automated accounts payable system). All staff have been trained as of January 25, 2024. This has been COMPLETED.</li> </ul>

# Summary of Findings



Finding #	Title of Finding	Rating	Management Response
4	Missing and unclear documentation supporting justification for use of Single and Sole Source Vendors.	Medium	<p>Agree. Administrative Services will:</p> <ul style="list-style-type: none"> <li>• Management agrees with Finding #4 of the Procurement of Goods Audit. The revised Policy and Manual will clearly outline criteria and the required supporting documentation to support the use of single and sole source vendors. This Policy will be in place by 6/30/2024 and effective 07/01/2024, Administrative Services will have direct oversight of LACERA's centralized vendor management program. This team will ensure compliance will all solicitation requirements.</li> </ul>
5	Insufficient documentation for excluding the lowest bidder in a three-bid process.	Medium	<p>Agree. Administrative Services will:</p> <ul style="list-style-type: none"> <li>• Management agrees with Finding #5 of the Procurement of Goods Audit. The revised Policy and Manual will include guidelines for selecting a bid if the lowest is not accepted including required supporting documentation. This Policy will be in place by 6/30/2024 and effective 07/01/2024, Administrative Services will have direct oversight of LACERA's centralized vendor management program. This team will ensure compliance will all solicitation requirements.</li> </ul>
6	Inefficiencies and discrepancies noted on the Forms Inventory Tracking Spreadsheets.	Low	<p>Agree. Administrative Services will:</p> <ul style="list-style-type: none"> <li>• LACERA Management agrees with Finding #6 of the Procurement of Goods Audit. Consistent with LACERA's values of collaboration and accountability, Management expects and has directed divisions to work cooperatively to agree upon an alternative means to track the inventory of forms to be used and updated by all impacted divisions. Agreement will be reached on the shared tool to track inventory of forms and impacted divisions will begin using that new tool by 06/30/2024.</li> </ul>

# Thank you



We would like to thank Administrative Services for their cooperation on this engagement and invite them to provide any comments.





March 5, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Christina Logan   
Principal Internal Auditor  
Nathan K. Amick   
Senior Internal Auditor

FOR: March 18, 2024 Audit Committee Meeting

**SUBJECT: 2024 Audit Committee Orientation**

The attached presentation provides each member with information about the Audit Committee and Internal Audit, and an overview of the professional standards that internal auditors adhere to.

In conjunction with the presentation, we have attached the current versions of LACERA's Audit Committee and Internal Audit Charters (Attachment A and B). The Committee last reviewed and approved the charters in 2021.

The Institute of Internal Auditors (IIA) released its updated standards, the [Global Internal Audit Standard](#), in January 2024, and they will become effective in January 2025. During this time, Internal Audit will be conducting a readiness assessment and address any gaps between the new standards and our current practices.

Attachments:

- A. LACERA Audit Committee Charter 2021
- B. LACERA Internal Audit Charter 2021

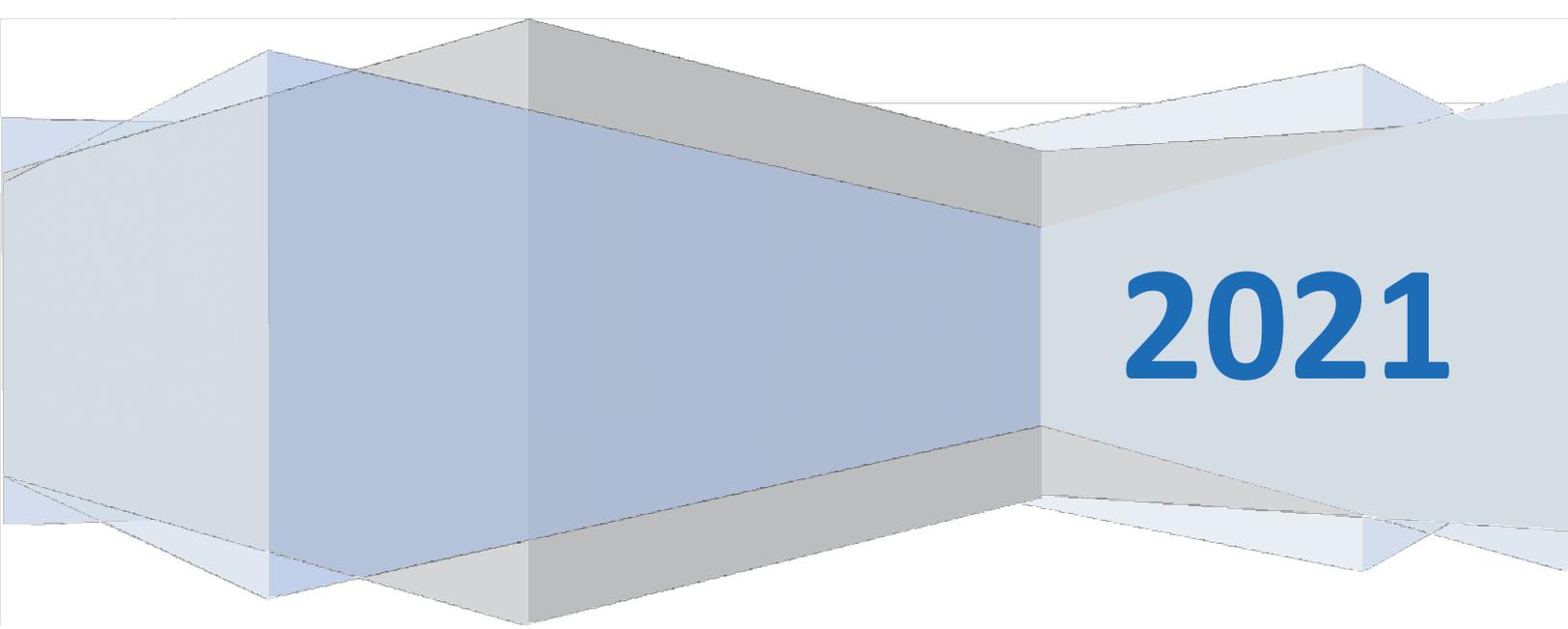
Noted and Reviewed:



Richard P. Bendall  
Chief Audit Executive

# Audit Committee Charter

**April 2021**



**2021**



**AUDIT COMMITTEE CHARTER**

**Table of Contents**

- I. CHARTER .....2**
- II. PURPOSE AND ASSIGNED FIDUCIARY OVERSIGHT DUTIES.....2**
- III. PRINCIPLES OF THE AUDIT COMMITTEE ..... 2**
- IV. AUTHORITY .....3**
- V. AUDIT COMMITTEE COMPOSITION AND CONSULTANT..... 3**
- VI. AUDIT COMMITTEE MEETINGS .....4**
- VII. RESPONSIBILITIES .....5**
- VIII. APPROVAL.....9**



## 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
- F. Audit Committee and Internal Audit Budget

### 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.

#### **V. AUDIT COMMITTEE COMPOSITION AND CONSULTANT**

The Audit Committee will consist of seven members: three elected annually from each Board and the ex-officio member of both Boards, the Los Angeles County Treasurer. If any elected Audit Committee member leaves Board service or resigns from the Audit Committee prior to the completion of his or her term, the Board of the departing member, will elect a new Audit Committee member at the next regularly scheduled Board meeting.

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 Chair, 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.

All meetings of the Audit Committee shall be as noticed as joint meetings with the Board of Retirement and Board of Investments to allow for participation of all trustees in open and closed session Audit Committee discussions, provided that non-committee trustees may not make or second motions or vote and provided further that closed sessions to discuss the CAE's annual assessment and the Committee's recommendation to the Boards regarding the appointment, discipline, dismissal, and/or removal of the CAE shall be noticed for attendance by Committee members only.

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 and also published on the LACERA website, [lacera.com](http://lacera.com). 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 the seven-member Audit Committee, 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. 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 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.
4. Resolve any significant disagreements regarding risks, findings and/or compensation between management and Professional Service Providers

#### **C. Financial Reporting Process**

The Audit Committee is responsible for oversight of the independent audit of LACERA's financial statements, 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. Audit Committee and Internal Audit Budget**

LACERA will provide appropriate funding, as determined by the Audit Committee, for compensation to the Financial Auditor, to any Professional Service Provider that the Audit Committee chooses to engage, and for payment of ordinary administrative expenses of the Audit Committee that are necessary or appropriate in carrying out its duties.

**G. 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 April 23, 2021, and approved by the Board of Retirement on July 7, 2021, and the Board of Investments on July 14, 2021. This Charter is thereby effective July 14, 2021 and is hereby signed by the following persons who have authority and responsibilities under this Charter.

*Joseph Kelly**July 19, 2021*


---

**Joseph Kelly**  
Chair, Audit Committee

---

**Date**

*Keith Knox**July 19, 2021*


---

**Keith Knox**  
Chair, Board of Investments

---

**Date**

*Alan Bernstein**July 19, 2021*


---

**Alan Bernstein**  
Chair, Board of Retirement

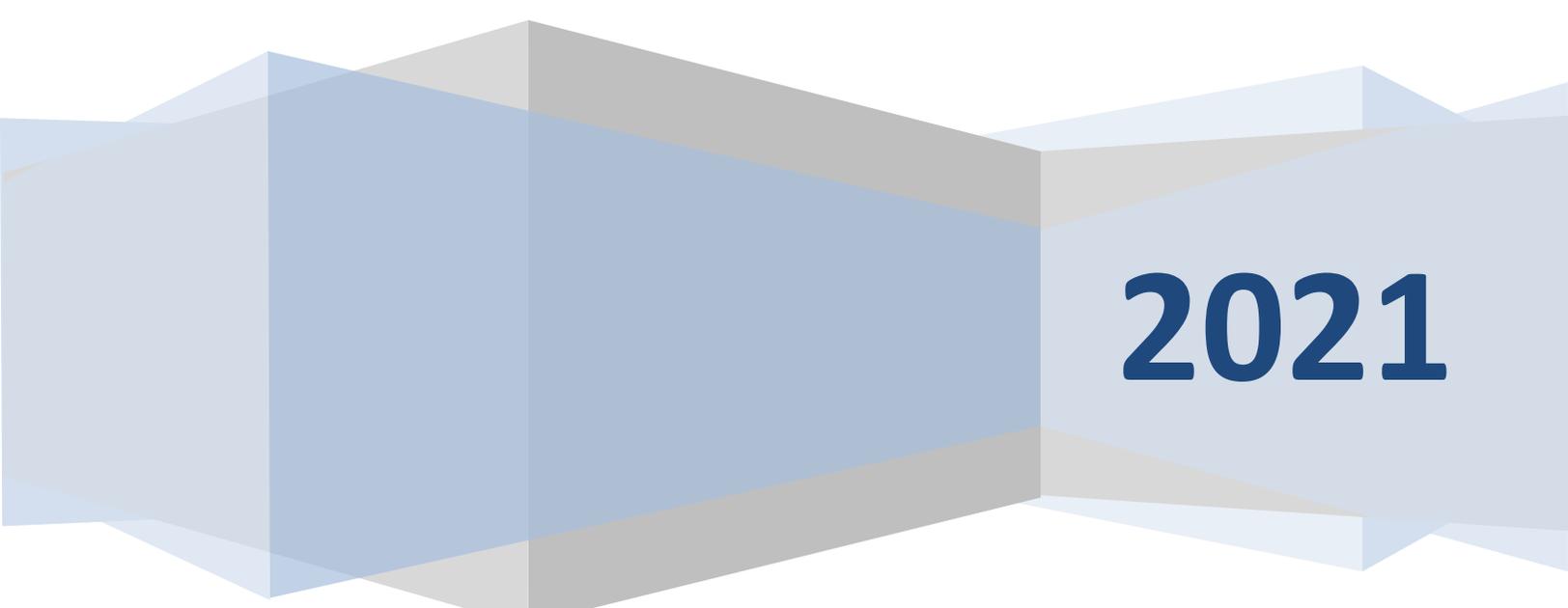
---

**Date**

# Internal Audit Charter

INTERNAL AUDIT SERVICES

August 2021



**2021**



---

**INTERNAL AUDIT CHARTER**

<b>I. PURPOSE AND MISSION.....</b>	<b>3</b>
<b>II. ROLE.....</b>	<b>3</b>
<b>III. OBJECTIVES.....</b>	<b>3</b>
<b>IV. STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING .....</b>	<b>4</b>
<b>V. ORGANIZATION .....</b>	<b>4</b>
<b>VI. AUTHORITY .....</b>	<b>4</b>
<b>VII. INDEPENDENCE AND OBJECTIVITY.....</b>	<b>4</b>
<b>VIII. SCOPE OF INTERNAL AUDIT ACTIVITIES.....</b>	<b>5</b>
<b>IX. ACCOUNTABILITY.....</b>	<b>6</b>
<b>X. QUALITY ASSURANCE AND IMPROVEMENT PROGRAM .....</b>	<b>7</b>
<b>XI. APPROVAL.....</b>	<b>8</b>



## 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 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 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.

## **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.
- 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 August 26, 2021 . 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:**

<i>Signature on File</i>	<u>09/15/21</u>	<i>Signature on File</i>	<u>09/15/21</u>
<b>Joseph Kelly</b> <i>Chair, Audit Committee</i>	<b>Date</b>	<b>Santos H. Kreimann</b> <i>Chief Executive Officer</i>	<b>Date</b>
 <i>Signature on File</i>	 <u>09/15/21</u>		
<b>Richard Bendall</b> <i>Chief Audit Executive</i>	<b>Date</b>		



# 2024 Audit Committee Orientation

---

Presented by:

Christina Logan, Principal Internal Auditor

Nathan K. Amick, Senior Internal Auditor



- Audit Committee
- Internal Audit
- Global Internal Audit Standards

In these times of rapid change and increased uncertainty, the need for the oversight role that audit committees play is as critical as ever. The most effective audit committees are engaged, executing their responsibilities with diligence, and this engagement significantly enhances the financial reporting output.

—Sagar Teotia, SEC Chief Accountant

# Purpose of the Audit Committee



Assist Boards in fulfilling fiduciary oversight duties:

Internal & External Audit Activity

Financial Reporting Process

Organizational Values & Ethics

Organizational Governance

Committee Authority includes:

- Oversee work of Internal and External Audit activity
- Select, oversee, and compensate External Financial Auditor
- Conduct or authorize investigation
- Unrestricted access to management, staff, and relevant information

# Principles of the Audit Committee



The Audit Committee will conduct itself in accordance with LACERA's Code of Ethical Conduct and core principles from the Institute of Internal Auditors (IIA) Code of Ethics.

Integrity

Independence  
& Objectivity

Confidentiality

Competency

Professional  
Standards

# IIA's Key Definition



- The IIA defines the **board** as “the highest-level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization’s activities and hold senior management accountable.
- The word “board” in the IIA *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an **audit committee**).



# Audit Committee Charter



The Audit Committee Charter establishes the authority and responsibilities of the Audit Committee, as assigned by LACERA's Board of Retirement and Board of Investments.

## Audit Committee Charter

- Defines the audit committee's purpose, authority, and responsibility
- Establishes the audit committee's responsibility and fiduciary oversight duties
  - Internal audit activity
  - Professional service provider activity
  - Financial reporting process
  - Values and ethics
  - Organizational governance

## Review & Approval of Charter

- Reviewed at least every three years
- Last reviewed by the Committee on April 2021
- Last approved by the BOR and BOI July 2021
- Planned realignment of Charter - June 2024

# Audit Committee Consultant



The Audit Committee hires an Audit Committee Consultant as the technical and financial expert to advise the Committee on audit and financial matters.

## Requirements for a Consultant

- Advanced degree and related certifications
- Prior experience advising Audit Committees
- Specific knowledge of '37 Act Pension Systems
- Broad knowledge of public pension and investment practices and emerging trends
- Knowledge of financial regulatory sources (GASB, GAAP, GAAS, etc.)
- Strong sense of corporate governance

## Current Consultant

Larry Jensen, Principal Audit & Risk Management Services

Approved by the Audit Committee in December 2023

- Contract expires December 2026, with an option to extend for two one-year terms

# Overview - Internal Audit Division



## Mission:

Enhance and protect LACERA's organizational values by providing risk-based and objective assurance, advice, and insight.

## Purpose:

Provide independent and objective assurance, consulting, and advisory services that are designed to add value and improve LACERA's operations.

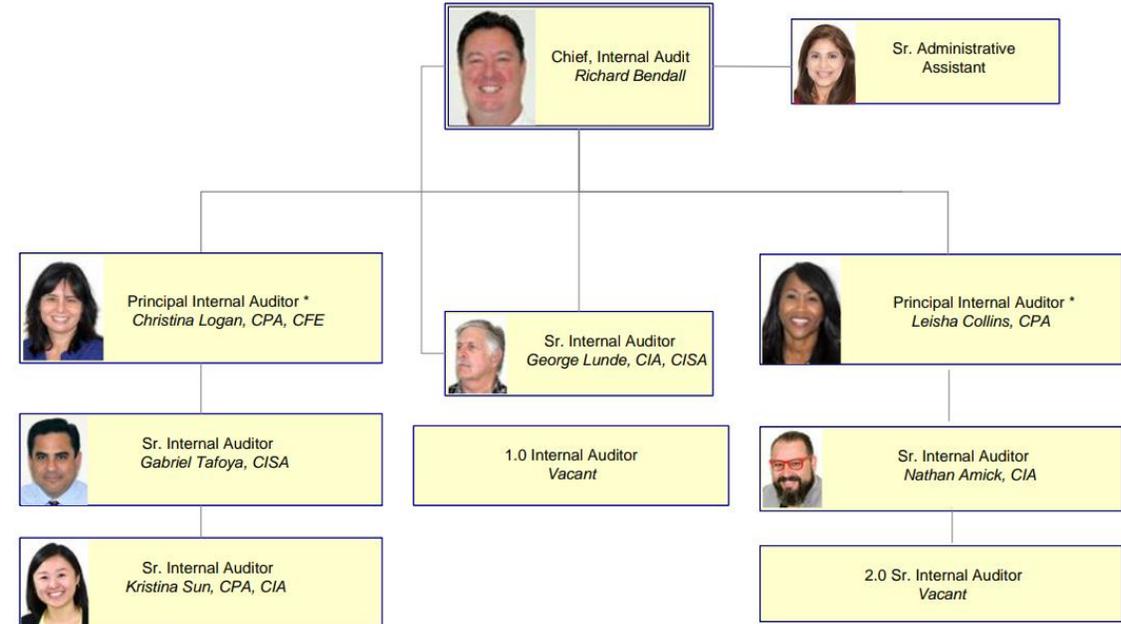
## Assurance / Audit Engagements

## Consulting Engagements

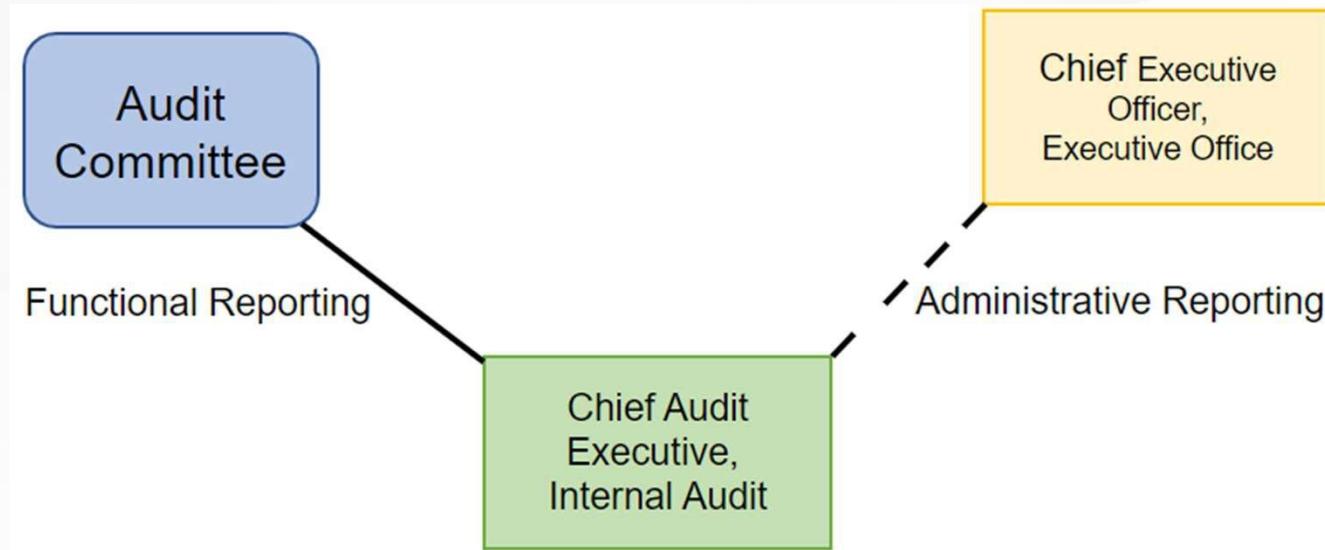
## Advisory Engagements

### The Internal Audit Team

### INTERNAL AUDIT FISCAL YEAR 2023-2024



# IA's Organizational Independence



Internal Audit reports functionally to the Audit Committee to ensure Management cannot unduly influence the nature or scope of audit work. Meetings are held to keep the Audit Committee abreast of Internal Audit's work, and risks and issues.

Internal Audit reports administratively to the Chief Executive Officer.

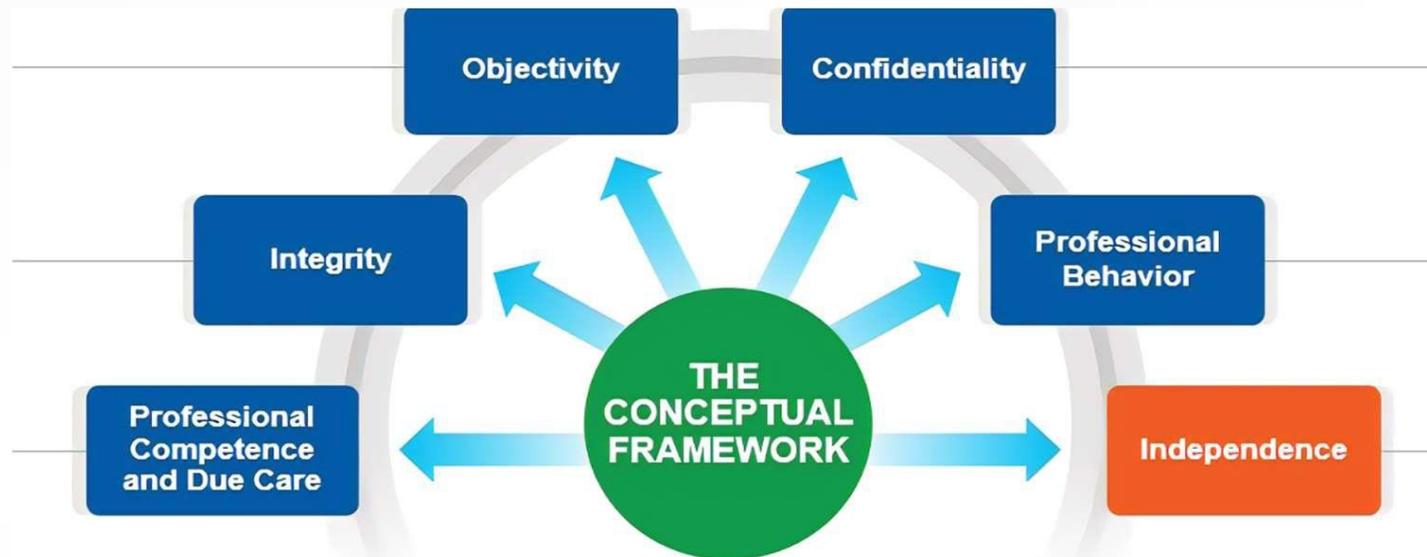
**Key Take-Away: Internal Audit is independent of operations.**

# Key Principles of Internal Audit



Internal Audit and its staff will conduct itself in accordance with LACERA's Code of Ethical Conduct and core principles from the Institute of Internal Auditors (IIA) Code of Ethics.

Annually, Internal Audit staff are required to attend a two-hour IIA Ethics course and acknowledge the IIA's Standards regarding Independence & Objectivity, Proficiency & Due Care, and the Code of Ethics. This was last completed in December 2023 with no exceptions.



# Internal Audit Charter



The IIA *Standards* 1000 and 1010 requires an internal audit charter to define the purpose, authority, and responsibility of internal audit activity and to recognize the mandatory guidance in the audit charter.

## Internal Audit Charter

- Defines the internal audit activity's purpose, authority, and responsibility
- Establishes the internal audit activity's position within the organization
- Defines the nature of the chief audit executive's functional reporting relationship with the board
- Defines the scope of internal audit activities

## Review & Approval

- Reviewed annually by staff and present changes to Committee when necessary
- Last reviewed by Audit Staff in 2023 – No changes were made because the IIA released revised standards in January 2024.
- Planned realignment of Charter in June 2024

# New Global Internal Audit Standards

- January 2024 - new [Global Internal Audit Standards](#) “Standards” were released.
- April 2024 – ensure Internal Audit understands new Standards and how it will impact our division.
- June 2024 – bring revised Audit Committee and Internal Audit Charters to Committee for review and approval.
- October 2024 – perform a self-assessment to gauge our readiness to conform.
- December 2024 – ensure gaps identified in self-assessment have been addressed.
- January 2025 – Standards become effective.



# Resources for Internal Auditors



- Association of Public Pension Fund Auditors (APPFA)
- American Institute of Certified Public Accountants (AICPA)
- Association of Certified Fraud Examiners (ACFE)
- Information Systems Audit and Control Association (ISACA)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)



# Questions or Comments





March 6, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Richard P. Bendall   
Chief Audit Executive

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Annual Audit Planning for Fiscal Year 2024-2025**

According to The Institute of Internal Auditor's (IIA) International Standard 2010 for Planning<sup>[1]</sup>, the Chief Audit Executive (CAE) must establish a risk-based plan to determine the priorities of the internal audit activity and ensure audit resources are appropriately allocated to address top priorities and key risk areas for the organization. Generally, audit plans are developed in three phases: define and refine the audit universe, assess the risks, and develop the plan.

We will be presenting our Audit Planning Process, including a discussion on current risks identified through external research and resources. Please find the following attachments related to this item:

#### Attachments

- A. Presentation slides on Annual Audit Planning for Fiscal Year 2024-2025
- B. 2024 Division Risk Survey
- C. The IIA's 2022 OnRisk Report
- D. The Internal Audit Foundation's 2024 Risk In Focus Report

<sup>[1]</sup> For IIA Standard 2010, refer to website at [www.globaliia.org/standards-guidance](http://www.globaliia.org/standards-guidance) or [www.theiia.org/guidance](http://www.theiia.org/guidance)



# Audit Planning for Fiscal Year 2024-2025

---

Presented by:

Richard P. Bendall, Chief Audit Executive



**Overview of Audit  
Planning**



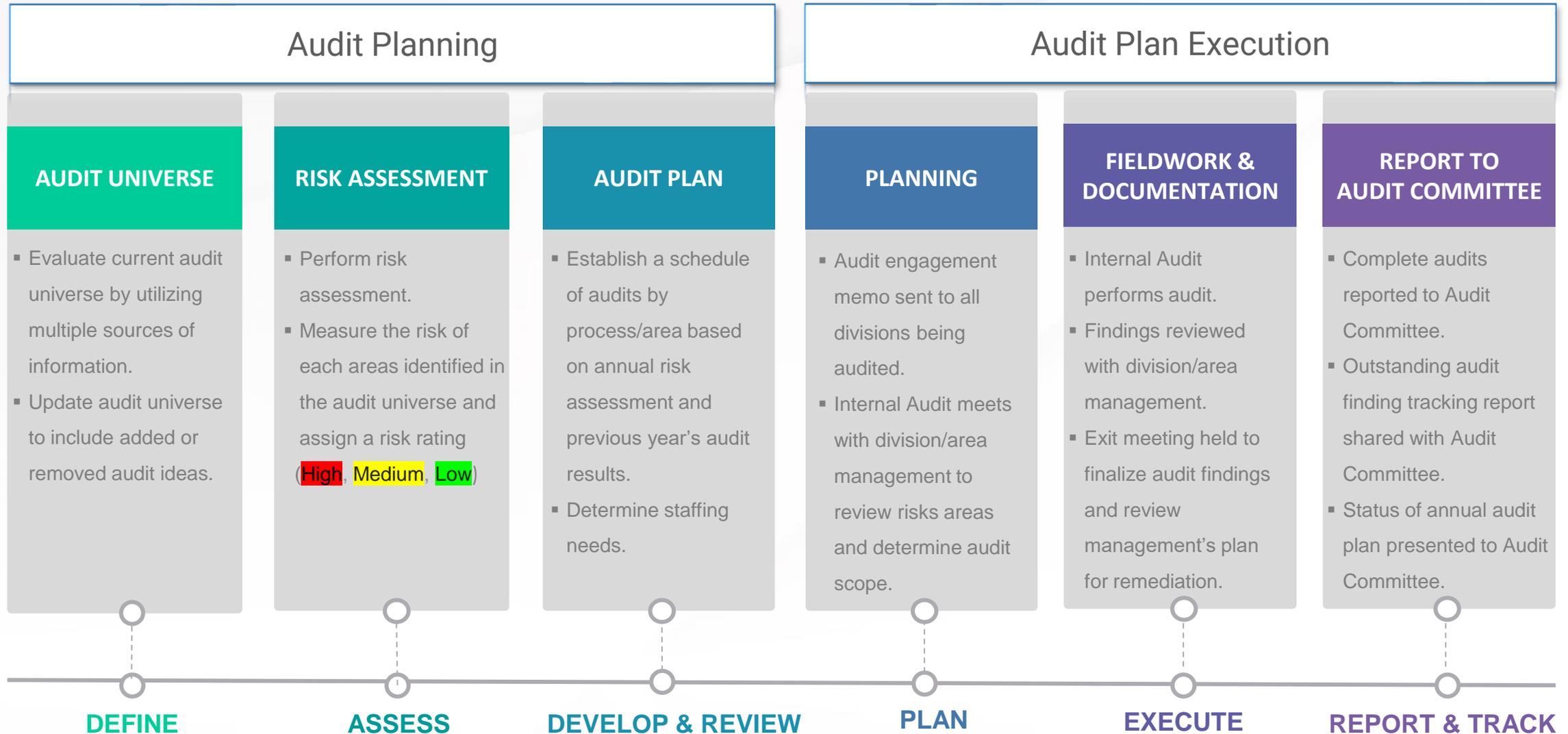
**Current Risks**







# Overview of Internal Audit Process



# Annual Audit Planning for FYE 2024



March Meeting



## Propose Audit Plan & Budget

Based on:

- Cyclical / known risk areas
- Review AC & IA Charters
- Review past audit findings & recommendations

## Define/Refine Audit Universe

Based on:

- Evaluate current risks in industry
- Evaluate recent organizational changes
- Evaluate if needed to update universe

## Complete Audit Universe & FYE 2023 Audit Plan

- With input from Executive Office and Audit Committee
- Committee Approval of Audit Plan

June Meeting

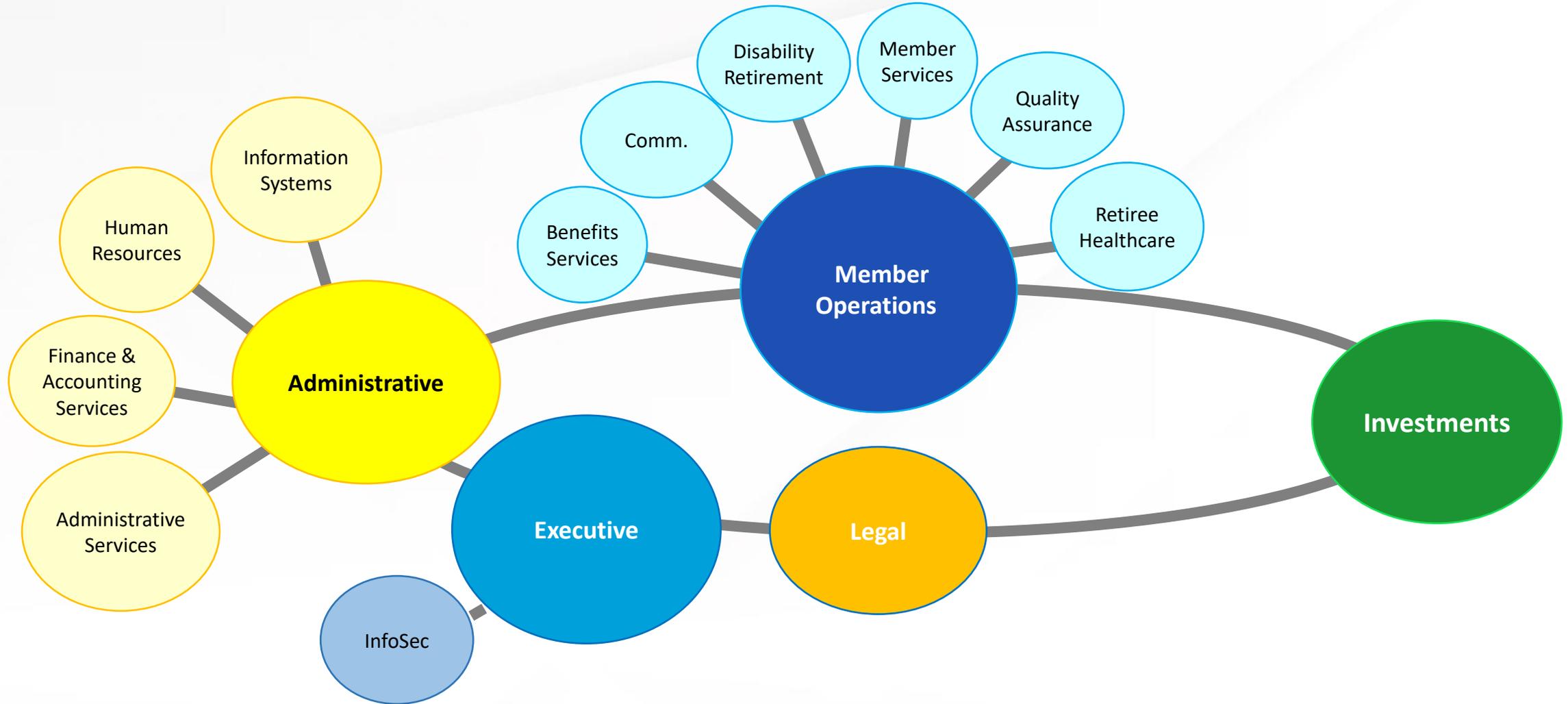


## Assess Risk

Based on:

- Understand the organization's risk areas
- Input from Audit Committee
- Review Division Budget Highlights
- Update divisional risk surveys
- Interview Division Managers and staff
- Assess the risk of each area identified in the audit universe

# Audit Universe by Organization Structure



# Snipit of 2024 Divisional Risk Survey



Internal Audit Division  
2024 Risk Assessment

<b>Division:</b>		<b>Survey Completed By:</b>		<b>Date:</b>	
------------------	--	-----------------------------	--	--------------	--

**Instructions:** Please answer the following questions to the best of your ability. When answering the questions, you should consider risks associated with work processed within your Division and controls implemented to address those risks.

<b>OPERATIONAL OBJECTIVES</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
1. Are key objectives/goals clearly established for your Division? List the key objectives/goals of your Division?			
2. Have you established key performance indicators (KPIs) for each objective. If yes, please list the KPIs associated with each objective. If the answer is no, please describe where you are in the process of developing KPIs.			
3. Are there significant operational limitations that prevent your Division from accomplishing your Divisional objectives? Describe at a high level.			
4. Are there any initiatives in LACERA's Strategic Plan that will have a significant impact on your			

# Current Risks





Published by the Institute of Internal Auditors (IIA) in December 2022

- Identified 12 key risks organizations face for 2022 and beyond
- Brought together key risk management players: Management/C-Suite, and Chief Audit Executives (CAEs)
- Focused on organizational knowledge, capability, and relevance related to each risk





2024 RISK IN FOCUS  
Hot topics for internal auditors

NORTH AMERICA

Read more

Internal Audit FOUNDATION

## ABOUT RISK IN FOCUS

**Risk in Focus provides practical, data-driven research to help internal auditors and their stakeholders understand today's risk environment and prepare audit plans for the year ahead.**

Reports are based on a worldwide survey to identify current and emerging risks for each region, followed up with roundtables and interviews to discover leading practices for internal auditors.

Each of The IIA's six regions will receive two reports:

- **Hot Topics for Internal Auditors** – Detailed reports based on the survey, roundtables, and interviews.
- **Board Briefing** – Summary reports for internal auditors to share with stakeholders.

Global Risk in Focus is a collaborative partnership facilitated by the [Internal Audit Foundation](#) with

generous support from IIA regional bodies, IIA Institutes, and corporate sponsors. 2024 marks the first year the project was conducted worldwide.

The Risk in Focus methodology was originally created in 2016 by the European Institutes Research Group (EIRG), which continues to publish it in Europe through the European Confederation of Institutes of Internal Auditing (ECIIA).

Reports are available free to the public at The IIA's [Risk in Focus resource page](#) and at the websites for IIA regional groups: [ACIIA](#) (Asia Pacific), [AFIIA](#) (Africa), [ARABCIIA](#) (Middle East), [ECIIA](#) (Europe), [FLAI](#) (Latin America).

# Top Risks per OnRisk & Risk in Focus Reports



Risk	Description of what the risk examines
Cybersecurity	Are organizations sufficiently prepared to manage cyber threats that could cause disruption & reputational harm
Human Capital	The challenges organizations face in identifying, acquiring, upskilling, and retaining the right talent to achieve their objectives.
Organizational Governance	Whether organizations' governance assists or hinders achievement of objectives.
Data Privacy	How organizations protect sensitive data in their care and ensure compliance to all applicable laws and regulations.
Culture	Do organizations understand, monitor, and manage the tone, incentives, and actions that drive the desired behavior.
Fraud	Organizations ability to prevent, detect and take corrective action related to fraud.
Change in Regulatory Environment	The challenges organizations face in a dynamic and ambiguous regulatory environment.
Supplier & Vendor Management	Organizations' abilities to select and monitor third-party relationships.
Disruptive Innovation	Whether organizations are prepared to adapt to and/or capitalize on disruption.
Financial Liquidity	Risk to an organizations financial condition arising from inability to meet contractual obligations.

# 2024 Risk and Our Current Audit Plan



Top Risk Areas	Audit Project
Cybersecurity	Application Security Review and Support of Information Security
Organizational Governance	Strategic Plan – Compliance and Enterprise Risk Management
Talent Management	Follow up on 2022 Review of HR Recruiting by Eide Bailey
Business Continuity & Crisis Management	Advisory Project included in FY 2024 Audit Plan

# Questions





## **INTERNAL AUDIT RISK ASSESSMENT QUESTIONNAIRE FYE 2023-2024**

### PURPOSE:

As part of Internal Audit's risk assessment process, we are issuing the attached Risk Assessment Questionnaire (Questionnaire) to all managers. The Questionnaire is one of the tools that Internal Audit uses to gauge risk and controls throughout the organization. We also use the Questionnaire for audit planning.

### HOW TO COMPLETE THE QUESTIONNAIRE:

- For each question, answer yes or no, and provide additional comments in the "Comment" Section of the Questionnaire.
- A copy of your most recently completed Questionnaire is provided as a reference. You can copy responses from your prior Questionnaire where applicable.
- Provide responses for each question. If certain sections of the Questionnaire do not apply to your Division activities, leave them blank and record N/A in the "Comments" box.

Please complete the Questionnaire and email it to Richard Bendall, Leisha Collins, and Christina Logan, with CC' to Perla Gonzalez by April 26, 2024

<b>Division:</b>		<b>Survey Completed By:</b>		<b>Date:</b>	
------------------	--	-----------------------------	--	--------------	--

**Instructions:** Please answer the following questions to the best of your ability. When answering the questions, you should consider risks associated with work processed within your Division and controls implemented to address those risks.

<b>OPERATIONAL OBJECTIVES</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
1. Are key objectives/goals clearly established for your Division? List the key objectives/goals of your Division?			
2. Have you established key performance indicators (KPIs) for each objective. If yes, please list the KPIs associated with each objective. If the answer is no, please describe where you are in the process of developing KPIs.			
3. Are there significant operational limitations that prevent your Division from accomplishing your Divisional objectives? Describe at a high level.			
4. Are there any initiatives in LACERA's Strategic Plan that will have a significant impact on your Division? If yes, list here.			
5. Are your Division's critical business processes addressed in LACERA's Business Continuity Plan? List your Divisions' critical business processes/functions.			
6. Are there any critical processes or functions within your Division for which you do not have an adequate work-around in the case of a disaster? If yes, please describe.			
7. Are there any delays or backlogs in processes performed in your Division? If yes, list backlogs and summarize reasons for delay.			
Are documented policies and procedures for all key business functions current? List significant processes or procedures that are <b>not</b> documented with written procedures.			
8. Are there any specific known control weaknesses or areas where controls could be further enhanced, (e.g., improved segregation of duties, documentation of reconciliations and/or approvals, etc.? If yes, please describe.			
9. Are there factors outside of your Division's control that impact your ability to meet your business objectives? If yes, please describe.			

PERSONNEL	YES	NO	COMMENTS
10. Do you currently have any vacancies in key positions? How long have these positions been vacant? Describe how these vacancies impact your Divisions' key objectives and completing work?			
11. Have there been any significant staffing changes in the past year? How did these staffing changes impact your Division?			
12. Do staff work overtime on a regular basis? Describe how overtime hours, and other special work requirements (on-call, shift premium) are reviewed and approved.			
SIGNIFICANT CHANGES	YES	NO	COMMENTS
13. Are there any regulatory changes to laws or new legislative mandates that will impact your Division? If yes, please list.			
14. Have there been any significant changes to business processes in your Division within the past year? If yes, please describe.			
PRIVACY & DATA MANAGEMENT	YES	NO	COMMENTS
15. Do you have written Divisional privacy policies or procedures? If yes, attach copy to this questionnaire.			
16. Do any vendors you oversee have access to LACERA confidential data (membership information or investment information bound by non-disclosure agreements)? If yes, comment on how you ensure the data is adequately maintained and protected?			
COMPLIANCE	YES	NO	COMMENTS
17. Are there adequate controls in your Division to ensure compliance with legal or regulatory requirements affecting your Division? If no, please describe.			
18. Do you have a process for ensuring vendor compliance to contract requirements?			
19. Describe any areas of noncompliance or concerns regarding compliance.			
20. Are there any other areas of compliance specific to your Division that concern you? If yes, please describe.			

OTHER	YES	NO	COMMENTS
21. Have any frauds, privacy issues or significant incidents occurred in your Division in the past year. How and to whom were these incidents reported?			
22. What concerns you most about your Division? What keeps you up at night?			
23. How would you rate, staff's understanding of internal controls and risks from 1 (low) to 5 (high)			
24. Provide suggestions on potential audit areas or audit risks in LACERA that you believe Internal Audit should consider.			

In answering these questions, I have reviewed risks associated with work processed within my Division, and controls established to address those risks.

\_\_\_\_\_  
Division Manager Signature

\_\_\_\_\_  
Date

# ON RISK

A GUIDE TO UNDERSTANDING, ALIGNING, AND OPTIMIZING RISK

2022



# TABLE OF CONTENTS

<b>Introduction</b> .....	<b>3</b>
<b>The OnRisk Approach</b> .....	<b>4</b>
<b>Top Risks, 2022</b> .....	<b>5</b>
<b>Key Observations</b> .....	<b>6</b>
<b>Key Observations Explained</b> .....	<b>7</b>
Notable variations in capability and relevance for certain risks.....	8
Significant gap in relevance and capability ratings on several risks.....	10
Risks to pay attention to going forward.....	11
Perceptions of risk relevance vary greatly across ESG components .....	14
Pandemic revealed opportunities to improve organizational risk management .....	16
Senior executives and boards desire broader scope for internal audit services .....	18
<b>Insights and Actions – Board</b> .....	<b>20</b>
<b>Insights and Actions – C-suite</b> .....	<b>22</b>
<b>Insights and Actions – CAEs</b> .....	<b>23</b>
<b>Methodology</b> .....	<b>24</b>
<b>How to Use This Report</b> .....	<b>25</b>
<b>Risk Stages Model</b> .....	<b>26</b>
<b>The Risks</b> .....	<b>28</b>
Cybersecurity .....	30
Talent Management .....	31
Organizational Governance .....	32
Data Privacy .....	33
Culture.....	35
Economic and Political Volatility .....	36
Change in Regulatory Environment.....	37
Supplier and Vendor Management.....	38
Disruptive Innovation.....	39
Social Sustainability.....	40
Supply Chain Disruption .....	41
Environmental Sustainability.....	42

# INTRODUCTION

*“How complicated and unpredictable the machinery of life really is.”*

— Kurt Vonnegut

---

**In the 18 months since the COVID-19 pandemic first shuttered the world**, organizations have learned to embrace the unexpected. Board members, C-suite executives, and chief audit executives — the key players in risk management — now know that low likelihood/high impact risks must be given greater consideration. This realization has jolted boards into greater awareness of risk management weaknesses, energized senior management to build more nimble and resilient organizations, and positioned internal audit to deliver broader value.

Indeed, the pandemic has spawned changes in how we see our trusted institutions, the value and priorities we place on our time, and our commitments to long-held social contracts about work, diversity, and the health of the world around us. It is too early for definitive answers to which of these changes will be fleeting or permanent. However, one thing is certain. This once-in-a-century test of core social, business, political, and economic beliefs will forge changes both subtle and profound.

While historic, the lingering pandemic and its related fallout is not the only factor likely to influence risk in 2022. Growth in social upheaval, a significant shift in regulatory attitudes at the federal level, continuing economic and political volatility, continuing effects of climate change, and the marked acceleration of environmental-, social-, and governance-related issues will combine to make the coming year one filled with unpredictability and opportunity.

*“COVID-19 has been a wake-up call for organizations to create a plan for the unexpected. These ‘Hollywood type’ risk scenarios are now something that should be discussed to some extent within organizations.”*

– C-suite, Technology

*“Risk today has become very volatile and random. You see these things occurring globally in the news and there seems to be less correlation between the cause and effect.”*

– Board, Retail

# THE ONRISK APPROACH

---

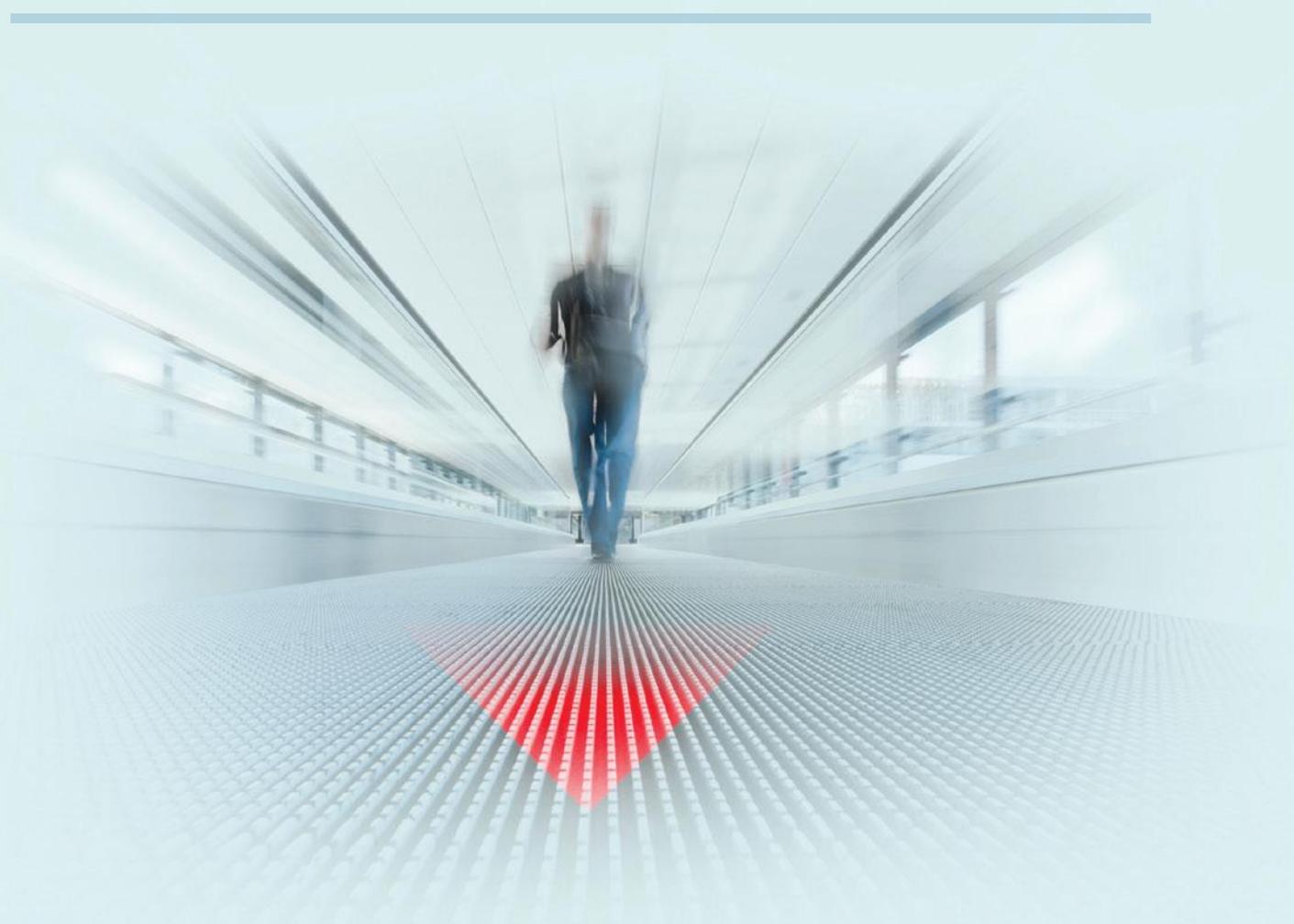
**The *OnRisk* approach is grounded in an innovative methodology** that uniquely brings together the perspectives of the major stakeholders in organizational governance — the board, executive management, and chief audit executives. Alignment of these stakeholders' views on personal knowledge, organizational capability, and risk relevance is a significant step toward achieving strong risk management in support of effective governance.

The methodology employs qualitative interviews of 30 board members, 30 C-suite executives, and 30 CAEs from 90 different organizations. The research provides a robust look at risks facing organizations and allows for both objective data analysis and subjective insights based on responses from risk management leaders.

Collective ratings for each group are assigned a value based on the percentage of respondents who rate particular aspects of each risk at a 6 or 7 on a 7-point scale. For example, if 7 in 10 board members rated their organizations' risk management capability on data privacy at a 6 or 7, the score would be 70%.

Further details regarding the *OnRisk* methodology, how to use and leverage this report, and explanations of the Stages of Risk developed in conjunction with the *OnRisk* approach can be found later in this report.

---



# TOP RISKS, 2022

The 12 risks below, carefully selected from a wide assortment of risks likely to affect organizations in 2022, were vetted through in-depth interviews with board members, executive management, and CAEs. Some of the risks included are unchanged from *OnRisk 2021*, some have been updated, while others have been added. For example, the 2021 risk for sustainability is broken out in 2022 to include Environmental Sustainability, Social Sustainability, and Organizational Governance. All of the risks in *OnRisk 2022* should have universal applicability to organizations, regardless of size, industry, or type. Risks not included in this analysis may have particular relevance to some organizations, depending on their specific circumstances. The risks are presented in order of relevance, as rated by *OnRisk 2022* respondents.

**CYBERSECURITY:** The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

**TALENT MANAGEMENT:** The increased need for and acceptance of remote operations, including working from home, as well as continued dynamic labor conditions, are redefining how work gets done. This risk examines the challenges organizations face in identifying, acquiring, upskilling, and retaining the right talent to achieve their objectives.

**ORGANIZATIONAL GOVERNANCE:** Governance encompasses all aspects of how an organization is directed and managed — the system of rules, practices, processes, and controls by which it operates. This risk examines whether organizations' governance assists or hinders achievement of objectives.

**DATA PRIVACY:** The growing list of regulations from jurisdictions around the world is making data privacy increasingly complex and dynamic. This risk examines how organizations protect sensitive data in their care and ensure compliance to all applicable laws and regulations.

**CULTURE:** With an increasing percentage of professional employees working remotely full or part time, organizations are challenged to maintain, enhance, or control their organizational culture. This risk examines whether organizations understand, monitor, and manage the tone, incentives, and actions that drive the desired behavior.

**ECONOMIC AND POLITICAL VOLATILITY:** The potential permanent impacts of the pandemic and the normal dynamics of macroeconomic cycles have the potential to create volatility in the markets in which organizations operate. This risk examines the challenges and uncertainties organizations face in a dynamic and potentially volatile economic and political environment.

**CHANGE IN REGULATORY ENVIRONMENT:** Fundamental changes in government appetite for regulation can have a significant impact on organizations, including those not considered heavily regulated. This risk examines the challenges organizations face in a dynamic and ambiguous regulatory environment.

**SUPPLIER AND VENDOR MANAGEMENT:** For an organization to be successful, it has to maintain healthy and fruitful relationships with its external business partners and vendors. This risk examines organizations' abilities to select and monitor third-party relationships.

**DISRUPTIVE INNOVATION:** We are in an era of innovative business models, fueled by disruptive technologies. This risk examines whether organizations are prepared to adapt to and/or capitalize on disruption.

**SOCIAL SUSTAINABILITY:** Increasingly, there is a recognition that organizations have significant influence on individuals who they employ, who work in their value chain, who consume their products and services, and who live in their communities. This risk examines the ability of organizations to understand and manage the direct and indirect impacts their actions have on individuals and communities.

**SUPPLY CHAIN DISRUPTION:** The disruption to business-as-usual operations globally, rooted in the global pandemic, has highlighted the need for resilience in supply chains in support of organizations' achievement of strategic objectives. This risk examines whether organizations have built in the flexibility to adapt to current and future supply chain disruptions.

**ENVIRONMENTAL SUSTAINABILITY:** Organizations are facing increased pressure from stakeholders, including shareholders, regulators, customers, and employees, to evaluate and disclose how they are impacting the environment in which they operate. This risk examines the ability of organizations to reliably measure, evaluate, and accurately report on their environmental impacts.

# KEY OBSERVATIONS

The qualitative interviews for *OnRisk 2022* provide a snapshot of how the principal drivers of risk management interact, which risks pose the greatest challenges to their organizations, and how alignment on risk management efforts impacts success. Analysis of the results identified six key observations that shed light not only into how risks are understood, but also how the ability to manage risk is perceived. In-depth examinations of these observations are found later in this report.

---

- **There are notable variations among risk management players on certain risks.** Overall, there is general alignment on organizational capability, risk relevance, and personal knowledge. However, there are noteworthy variations in several key risk areas.
  - **Significant gaps exist between risk relevance and organizational capability ratings on several risks.** The gap between how risk management players rate risk relevance versus organizational capabilities is alarmingly wide for Talent Management, Disruptive Innovation, Data Privacy, Cybersecurity, and Culture.
  - **Risks to pay attention to going forward.** Five risk areas emerged as top of mind for respondents: Cybersecurity, Talent Management, Culture, Disruptive Innovation, and Economic and Political Volatility. Of note, four of the five also had the largest gaps between risk relevance and organizational capabilities, suggesting risk players know where work needs to be done.
  - **Perceptions of risk relevance vary greatly across ESG components.** While alignment among the three groups is relatively strong on these risks, Organizational Governance holds far greater relevance for respondents than do Social Sustainability and Environmental Sustainability.
  - **The pandemic revealed opportunities to improve organizational risk management.** COVID-19 may not have improved the ability to predict risks, but it increased confidence for many in reacting to risks. For others, it provided a wake-up call on how they manage risk and the added challenges associated with managing risk in decentralized or siloed conditions.
  - **Senior executives and boards desire broader scope for internal audit services.** Respondents feel that their current assurance services are adequate but suggest some improvements in assurance reporting. This offers an opportunity to demonstrate the value of independent assurance across a wider spectrum of risks.
-

# KEY OBSERVATIONS EXPLAINED

.....  
.....  
.....  
.....  
.....

**The six key observations are examined in depth in the following pages.** As noted previously, the qualitative interviews for *OnRisk 2022* were designed to elicit candid perspectives on the nature and understanding of risk management through the eyes of its three principal drivers. The analysis and examination of those views reveal important insights into interactions and alignment among respondents and informative conclusions about how those interactions and alignments impact risk management.

.....  
.....  
.....  
.....



# NOTABLE VARIATIONS IN CAPABILITY AND RELEVANCE FOR CERTAIN RISKS

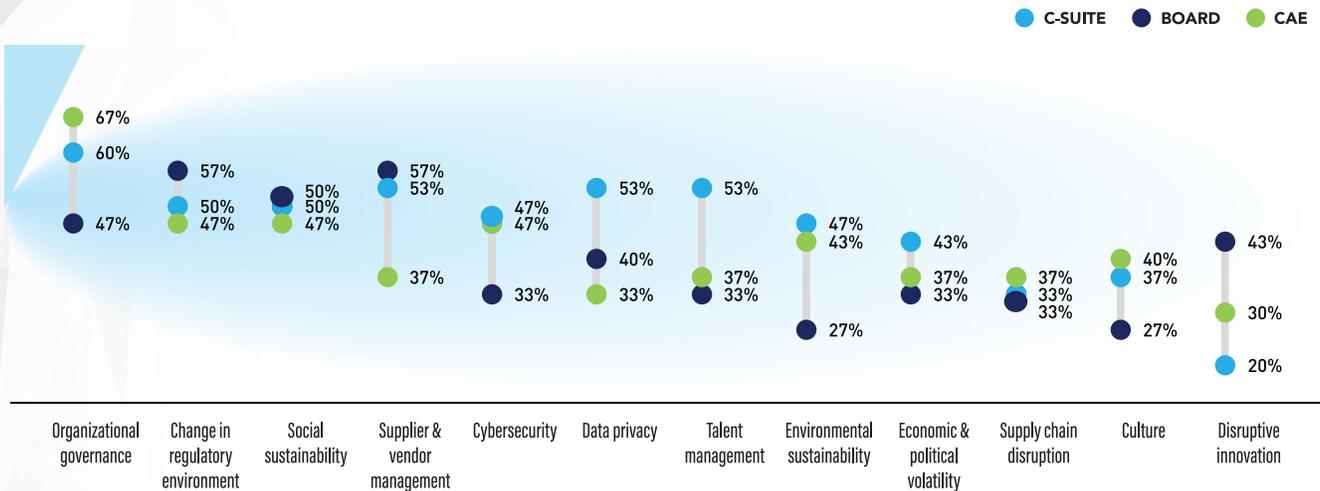
While overall ratings from the three respondent groups appear to reflect general alignment, deeper analysis of organizational capability and risk relevance ratings for each group finds noteworthy variations in several risk areas, particularly Disruptive Innovation.

Senior executives tended to be more confident about organizational capability for most risk areas examined except for Disruptive Innovation, where just 2 in 10 respondents rated capability as high (Figure 1). This created the largest variation between two respondent groups on capability — 23 percentage points between the C-suite and the board.

Boards are not as confident as senior executives on their organization’s capability to manage certain risks. For Talent Management and Environmental Sustainability, the capability rating was 20 points lower for board respondents compared to their C-suite counterparts. It was 13 points lower for Organizational Governance.

Meanwhile, CAEs were less confident in their organization’s ability to address Supplier and Vendor Management risk. Their ratings were 20 points lower than board respondents and 16 points lower than the C-suite.

**Figure 1:**  
**ORGANIZATIONAL CAPABILITY RATINGS BY ROLE PER RISK AREA**  
Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



**Note:** OnRisk 2022 interview question: Overall, how capable is your company when it comes to handling enterprisewide risk? Respondents could choose a rating from a scale of 1 to 7, with 1 being the lowest (“not at all”) and 7 being the highest (“extremely”). Risk areas were sorted from highest to lowest average scores. n = 90.

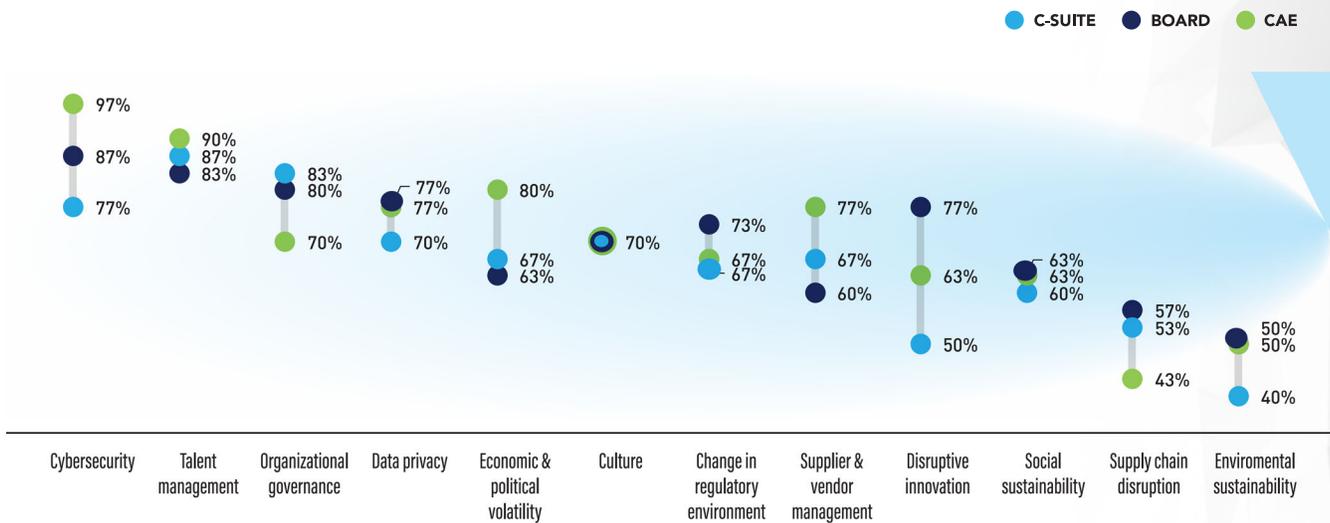
Similar variations were noted in risk relevance ratings (Figure 2). Boards were significantly more likely to rate Disruptive Innovation as a highly relevant risk (77%) than were senior executives (50%). This 27-point variance was the greatest between any two respondent groups in the risk relevance ratings.

Nearly every CAE (97%) rated cybersecurity as a highly relevant risk to their organization, but board respondents lagged by 10 percentage points (87%) and the C-suite lagged by 20 percentage points (77%). CAEs also were more likely to describe Supplier and Vendor Management as highly relevant — 17 points higher than the board and 10 points higher than the C-suite. A similar 17-point difference is noted between CAE and board ratings for Economic and Political Volatility.

**Figure 2:**

**RISK RELEVANCE RATINGS BY ROLE PER RISK AREA**

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



**Note:** OnRisk 2022 interview question: How relevant are each of the following risks to your current organization? Respondents could choose a rating from a scale of 1 to 7, with 1 being the lowest (“not at all”) and 7 being the highest (“extremely”). Risk areas were sorted from highest to lowest average scores. n = 90.

# SIGNIFICANT GAP IN RELEVANCE AND CAPABILITY RATINGS ON SEVERAL RISKS

While some ratings variation among individual respondent groups was expected, an analysis of the combined ratings for the three respondent groups uncovered additional insights. The analysis identified large gaps between higher risk relevance and lower organizational capability in several areas. This Relevance-Capability Gap reflects potentially significant risk management vulnerabilities.

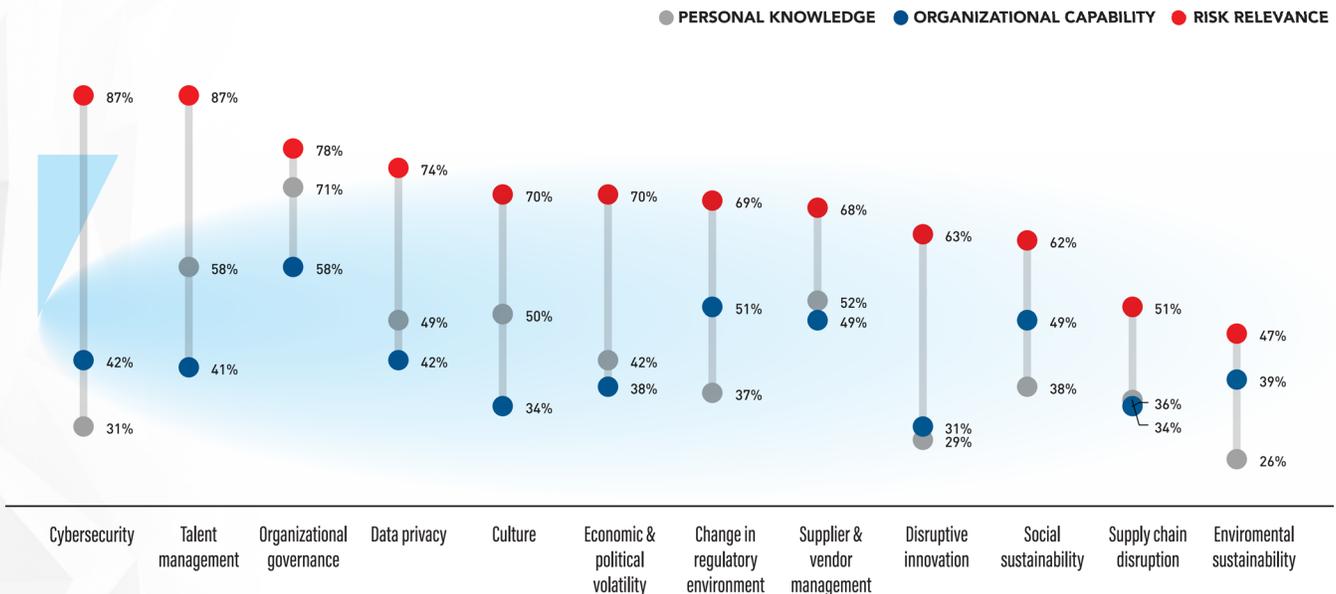
Chief among these is Cybersecurity, which continues to exasperate organizations large and small, public and private, for-profit and nonprofit. This ubiquitous and dynamic risk was rated as the most relevant by respondents, along with Talent Management (Figure 3). Yet, on average, organizational capability lagged significantly. Large disparities also are noted for Talent Management, Disruptive Innovation, Culture, Data Privacy, and Economic and Political Volatility.

For these risks, the relationship between relevance and capability varies. A highly relevant risk may be more difficult to manage because it is unpredictable and not easily controllable, due to, for example, external factors that may augment risk velocity. This appears to be the case for three of the six risks with the largest disparities: Cybersecurity, Disruptive Innovation, and Economic and Political Volatility. However, for Talent Management, Culture, and Data Privacy — risks that can be managed internally through controls and processes — the gaps may reflect more uncertainty coming out of the pandemic rather than a lack of control.

*“As we have witnessed with the pipeline hack this year, these cybersecurity attacks can have a huge trickle-down effect. All industries are susceptible to cybersecurity risk to some extent.”*

– Board, Manufacturing

**Figure 3:**  
**AVERAGE RATINGS PER RISK AREA**  
Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



**Note:** OnRisk 2022 interview questions: How knowledgeable are you about each of the following risks? How relevant are each of the following risks to your current organization? Overall, how capable is your company when it comes to handling enterprisewide risk? Respondents could choose a rating from a scale of 1 to 7, with 1 being the lowest (“not at all”) and 7 being the highest (“extremely”). All respondents. n = 90.

For example, the Relevance-Capability Gap for Talent Management may reflect uncertainty as organizations emerge from nearly 18 months of pandemic-induced isolation. This unease about workforce management ranges from the challenge of devising effective return-to-work strategies to more profound changes in the employer/employee social contract.

One healthcare C-suite executive credited the pandemic for an epiphany in this area. “The biggest thing on our minds right now is dealing with remote work and getting some of our employees back into the office, getting vaccinated, etc. The pandemic has definitely shown me that I was too rigid in my thought process in terms of remote work risk.”

Respondents expressed different approaches to managing risks that they cannot directly influence. For example, one financial company board member noted regulatory change is one that is relevant and carefully monitored, but largely out of the organization’s control. “Change in regulatory environment, for example, is very important to us. We’re very careful about the way that regulations affect us. It’s hard to do, and it’s not something anyone can really control.”

Meanwhile, a board member at a different financial services company said the firm chooses to focus on what can be governed. “We pay attention to risks that we can control. There is an importance of understanding your market and competitors when considering relevant risks that we might have less control over.”

As noted earlier, there is general alignment in personal knowledge, organizational capability, and risk relevance ratings among the respondent groups. However, the variance between relevance and capability is clearly evident in average ratings assigned by each respondent group (Figure 3).

## RISKS TO PAY ATTENTION TO GOING FORWARD

**Respondents identified five risks they expect to increase in relevance** in the next three to five years: Cybersecurity, Talent Management, Disruptive Innovation, Culture, and Economic and Political Volatility. Each of these fall into risk areas identified as having large Relevance-Capability Gaps. This concurrence could be viewed as troubling — organizations have fallen far behind on their capabilities to manage future risks — or encouraging — risk players intuitively recognize capability weaknesses and understand they must act to correct them.

**CYBERSECURITY:** The 45-point Relevance-Capability Gap for Cybersecurity (see Figure 3) reflects the near-constant struggle to keep up with the evolving and vexing nature of cyber risks. Cyber hackers are constantly looking for new weaknesses to exploit and novel ways to cash in on their criminal behavior. Ransomware and other denial-of-service type attacks are growing in number and sophistication, and the consequences are having broader impacts, as reflected in the cyberattack that temporarily halted operations of a major U.S. oil distribution system in May of 2021.

**TALENT MANAGEMENT:** Talent Management is expected to remain a top risk for the foreseeable future. At 46 points, this risk had the largest Relevance-Capability Gap of all risks examined this year, edging out Cybersecurity. Concerns about the pandemic’s impacts on the labor market and the traditional employer/employee social contract continue to keep this risk front and center in the minds of risk managers.

As noted in *OnRisk 2021*, “This significant disruption to talent management, as well as its impact on morale, productivity, and workplace culture, will have both short- and long-term implications for organizations.” Two areas offered as evidence of potential disruption have quickly come to fruition.

The work-from-home phenomenon fundamentally changed how organizations recruit and manage talent. While having a majority of the workforce operating in remote settings posed significant immediate challenges in technology, cybersecurity, and logistics, it all but eliminated the limitation of geographic considerations when identifying and hiring the right talent. As one manufacturing C-suite executive noted, “Talent management might become more challenging with the different generational gaps now becoming emphasized in the workforce. Where are we going to find the best talent?”

# RISKS TO PAY ATTENTION TO GOING FORWARD

(Continued)

Yet, the work-from-home experiment also appears to have had a profound impact on attitudes about work/life balance among various parts of the labor force. According to a June 2021 article in *Forbes* magazine<sup>1</sup>, expectations for many have changed in the year spent working from home. For instance, the article notes evidence that many are reconsidering career paths, citing increases in law and medical school applications jumping 20% and 18%, respectively.

A growing number of employees are leaving their jobs voluntarily. Dubbed “The Great Resignation,” this fallout from the pandemic promises to have long-term effects on the workforce. The United States saw nearly 4 million people quit their jobs in April 2021 alone, according to U.S. Bureau of Labor Statistics data, the largest single-month spike on record. Another 3.6 million left their jobs voluntarily in May. The phenomenon is not limited to the United States.<sup>2</sup>

According to the BBC<sup>3</sup>, a Microsoft survey of more than 30,000 global workers showed that 41% of workers were considering quitting or changing professions this year. The same report found a five-fold increase in remote job postings on LinkedIn since the start of the pandemic and that more than 46% of workers say they plan to move because they feel they can now work remotely.<sup>4</sup>

As organizations focus on getting workers back into office settings, they should carefully weigh the tightening labor market and how it relates to worker expectations in salaries, benefits, and work/life balance.

**CULTURE:** The distributed workforce created by the pandemic is feeding significant concern about workplace culture. The Relevance-Capability Gap for this risk is 36 points.

Building or sustaining a company culture virtually poses significant challenges, and organizations now face the question of whether to return to pre-pandemic work arrangements or find ways to adapt to greater percentages of offsite workers. The work-from-home experience has led to positive changes, including organizations witnessing increased trust, a flattening of hierarchies, and more rapid and agile decision-making. Yet, logistical challenges with communication, worker interaction, collaboration, fostering relationships, and consensus-building remain. Fundamental shifts in the employee/employer social contract (see section on talent management) further complicate this vexing risk.

**ECONOMIC AND POLITICAL VOLATILITY:** The continuing political and economic fallout from the pandemic drives this risk, pushing its Relevance-Capability Gap to 32 points.

According to a July 2021 U.S. Congressional Research Service report, emergence from the pandemic will be uneven globally, meaning continued economic volatility, particularly in developing countries.

“The economic impact of the pandemic is expected to lessen in developed economies where vaccinations are facilitating a return to pre-pandemic levels of activity. In developing countries, however, outbreaks of new viral variants could prolong the pandemic and dampen prospects of a recovery,” according to the report.

What’s more, a resurgence of COVID-19 cases brought on by new virus variants could prolong or create temporary setbacks in the recovery.<sup>5</sup>

*“We all ‘live’ culture, but understanding how to manage it and change it is a different beast altogether.”*

– CAE, Finance

*“Things were a breeze until 2008-2009. Now 2020-2021 into 2022, we’re expecting a lot of volatility...I don’t have strong feelings about where the economy is going, but we’re planning more now for major impacts like product shortages, delays, disruptions like that.”*

– C-suite, Finance

1: Kreznar, Christian, “Employers, Don’t Fear The ‘Great Resignation’—It’s Already Here,” *Forbes*, June 3, 2021.

2: Economic News Release, “Table 4. Quits levels and rates by industry and region, seasonally adjusted,” U.S. Bureau of Labor Statistics, Washington, D.C., <https://www.bls.gov/news.release/jolts.t04.htm>

3: Morgan, Kate, “The Great Resignation: How employers drove workers to quit,” BBC, July 1, 2021.

4: Microsoft 2021 Work Trend Index, <https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work>

5: “Global Economic Effects of COVID-19,” U.S. Congressional Research Service, July 9, 2021, Washington, D.C.

Historically, political volatility has followed economic shocks, most recently in the wake of the 2007-2008 international financial crisis. In April, International Monetary Fund Managing Director Kristalina Georgieva warned that preexisting inequalities that have been exacerbated by the pandemic might lead not only to macroeconomic instability, but also greater polarization, the erosion of trust in governments, and growing social unrest.<sup>6</sup>

**DISRUPTIVE INNOVATION:** Disruptive Innovation presents one of the greatest risk management challenges for organizations, which is reflected in the considerable misalignment between boards and the C-suite as it relates to risk relevance and organizational capability. This also contributes greatly to the overall 32-point gap between risk relevance and organizational capability for the combined respondent ratings. Frustration at the board level is evident. Some respondents recognize they are not prepared for managing such challenges, including one healthcare board member who said, “We’re not innovative, change is very slow to happen. Everything is about bandaging... a preparedness and ability to adapt is not there.”

A retail board member expressed frustration relating to not being able to see beyond the risk horizon. “If we knew what [the disruptive innovation] would be, we would be working on it. But we don’t know what is coming.” However, the movement among senior executives toward building organizations that are more nimble and responsive to fast-moving and emerging risks could contribute to improvements in this risk area. The Netflix vs Blockbuster story provides a stark example of how recognizing and leveraging disruption can mean the difference between spectacular success and stunning failure.

Blockbuster pioneered and dominated video rental services through a vast network of brick-and-mortar stores. Indeed, it dismissed an offer to merge with the Netflix mail-order video service in 2000. However, just six years later, Netflix dominated online video rentals, with 6.3 million subscribers compared to 2 million subscribers for Blockbuster. In 2008, Netflix leadership again showed that it recognized how technology could disrupt its business model significantly and responded. It signed a deal to stream movies for Starz, and by 2010, it held a 20% share of North American viewing traffic after signing additional deals with Sony, Paramount, Lionsgate, and Disney. That same year, Blockbuster filed for bankruptcy.

<sup>6</sup>: Hammond, Andrew, “The world is facing even greater political upheaval in post-pandemic world,” *Arab News*, April 8, 2021.

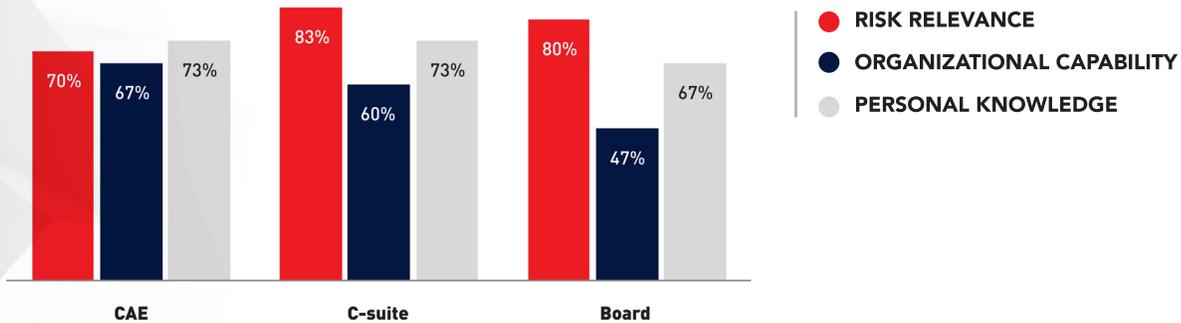


# PERCEPTIONS OF RISK RELEVANCE VARY GREATLY ACROSS ESG COMPONENTS

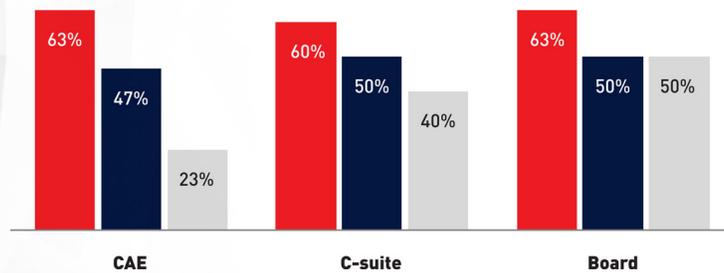
**OnRisk 2022 breaks out the three risk areas associated with ESG** — Environmental Sustainability, Social Sustainability, and Organizational Governance. Respondent ratings and responses clearly indicate Organizational Governance dominates over Social Sustainability and Environmental Sustainability in the minds of survey participants (Figure 4). In all three *OnRisk* measures — personal knowledge, organizational capability, and risk relevance — respondents rank Organizational Governance among the highest of all risks examined and well ahead of Social Sustainability and Environmental Sustainability risks.

**Figure 4:**  
**ESG MEASURES – COMPARING RELEVANCE, KNOWLEDGE, AND CAPABILITY TO ROLE**  
 Percentage who gave a rating of 6 or 7 on a scale of 1 to 7

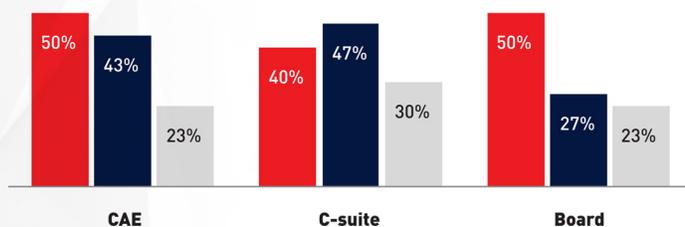
## ORGANIZATIONAL GOVERNANCE



## SOCIAL SUSTAINABILITY



## ENVIRONMENTAL SUSTAINABILITY



**Note:** *OnRisk 2022* interview questions: How knowledgeable are you about each of the following risks? How relevant are each of the following risks to your current organization? Overall, how capable is your company when it comes to handling enterprisewide risk? Respondents could choose a rating from a scale of 1 to 7, with 1 being the lowest (“not at all”) and 7 being the highest (“extremely”). n = 90.

This high ranking may be influenced by the broad relevance of Organizational Governance. Indeed, most organizations recognize the need and value of having strong risk controls across a spectrum of risks that affect the achievement of goals. It also may reflect often heroic and aligned efforts to respond to governance challenges created by the pandemic and the need for strong leadership to overcome those challenges. Further, it indicates a growing awareness of the benefits of risk alignment among key risk management players, which supports stronger organizational governance.

One manufacturing C-suite executive linked alignment with success. “We came to the conclusion that we were aligned... It showed how we are in line with most things, which I think helps us be successful.” Other comments reflect a growing awareness of the value of strong organizational governance and the dangers of weak governance:

*“For a lot of public companies, capability could be higher. Just look at some of the issues that arise...if everyone was really good at it, we wouldn’t be seeing so much breakdown in the structures at public companies.”*

– Board, Finance

*“We’ve now created a separate risk committee amongst our board. This has helped us to end up with some great documents regarding our organization’s handle on different risks.”*

– Board, Finance

*“How you plan for all of the other risks can be [attributed] to organizational governance... it’s extremely important and covers everything.”*

– Board, Finance

(See additional analysis of how the pandemic revealed opportunities to improve organizational risk management on page 19)

Advocates of corporate sustainability are quick to point to social and environmental sustainability being critical components to overall sound organizational governance. However, risk relevance rankings by *OnRisk* respondents did not reflect such clear associations. Indeed, Social Sustainability and Environmental Sustainability ranked in the bottom quartile in risk relevance. Despite widespread concern about climate change, fewer than half of respondents identified Environmental Sustainability as a highly relevant risk within their organizations. To be sure, comments from some respondents reflected a narrow scope of context relating to environmental sustainability.

*“People at our work eat, drink, use the bathroom, but we’re not producing toxins that they have to dump somewhere, so it’s not something that enters the conversation.”*

– C-suite, Technology

There has been growing awareness of ESG risks — as reflected in the growing number of organizations producing ESG reports and growing investor pressure for such reporting — but changes appear as likely to be driven by short-term considerations versus fundamental recognition of sustainability’s value. For example, Social Sustainability has become a focal point in the last 18 months due to global events and growing social activism, but Environmental Sustainability still lags.

Respondents believe a mix of real and artificial change is occurring and most think their organization is driving real change. However, comments from some respondents reflect a mix of short-term consideration and parochial mindsets.

One manufacturing C-suite executive associated the ESG movement more with marketing than with overall sustainability. “We have to have enough awareness to get through the door, get this bid, and get the job, but so far it seems like more of a gimmick for customers than a real market driven desire.”

However, others understand the value of managing environmental impacts, including a healthcare industry board member who lamented that such considerations must compete with other risks. “Most organizations want to have good environmental sustainability policies, procedures, and programs, but it is not always front and center when dealing with all these other risks.”

# PERCEPTIONS OF RISK RELEVANCE VARY GREATLY ACROSS ESG COMPONENTS

(Continued)

Other respondents expressed a more expansive view and understanding of how ESG components can work in concert within an organization.

*“Sustainability is going to be an absolute imperative in order to preserve, maintain, and grow wealth. This is like any other investment in business. These investments need to be made in order to protect and sustain the value that’s being created.”*

– Board, Finance

*“We need to have leaders that are open-minded to social sustainability change, that are willing to change and put in the work, or else change isn’t going to happen.”*

– CAE, Education

Organization size and maturity also were cited as potential limits to managing ESG risks. Limited resources make ESG risks — particularly those relating to E and S — lower priorities.

One C-suite executive from a nonprofit lamented, “I wish that we could be better with ESG, but it’s just not a priority. We’re a small business, so things like cybersecurity, organizational governance take precedence and environmental and social sustainability take the backseat. Some organizations are fortunate enough to have a team dedicated to ESG or even an employee working on it, but we’re stretched too thin as it is.”

The lack of clear direction or standards for measuring and reporting ESG also was cited as a deterrent. According to one finance CAE, “Having some sort of measurement for ESG would help to drive real change. You need to be taken accountable and show that real things are happening, and then also document and report on what is happening.”

However, a manufacturing industry CAE believes that companies that focus too much on reporting are missing the real benefit of ESG risk management. “The problem is that companies focused on reporting could be more artificial... they could be just checking the box, putting out reports to say they did it so that their stakeholders are happy. There needs to be more initiatives and actual activity occurring.”

## PANDEMIC REVEALED OPPORTUNITIES TO IMPROVE ORGANIZATIONAL RISK MANAGEMENT

**COVID-19 forced most organizations to focus to some degree** on how risk management efforts are aligned across their organizations. The pandemic may not have improved their ability to predict risks, but it increased confidence for many in reacting to risks. For some, it provided an opportunity to assess or reassess resilience. For others, it provided a wake-up call on how they manage risk and the dangers of decentralized or siloed conditions.

One nonprofit board member described how the pandemic proved to be eye-opening. “It has made us aware that there are scenarios that might happen in the future that we have to manage, and now we’re hyper aware of shortfalls of our risk approach.”

A retail industry board member, meanwhile, saw the good and bad in the pandemic-induced introspection. “It showed us that we weren’t really good at predicting risk, but I think we reacted very well. It made us aware of scenarios that might happen in the future and how we will handle them.”



# PANDEMIC REVEALED OPPORTUNITIES TO IMPROVE ORGANIZATIONAL RISK MANAGEMENT

(Continued)

*OnRisk* respondents also expressed concerns about alignment with third-party providers and partners. According to one education CAE, “There is the concern that third parties are not aligned on objectives, reporting, especially with risks like cybersecurity. Organizations should improve how they monitor third-party agreements, contract management, relationship building...a lot of time they’re just ‘getting it done,’ and not reflecting.”

As the world slowly emerges from more than a year of shuttered economies, homebound workforces, strained or disrupted supply lines, and sobering death tolls that top 4 million globally, early focus on post-COVID-19 risk management appears to be primarily short-term concerns.

“It definitely has impacted our perspective when it comes to risk. But I don’t think we have any concrete plans in place to change our risk strategy or anything long term yet. We’re focusing on getting our hybrid system set up and maintaining the health and safety of our employees,” said one government sector CAE.

Meanwhile, one technology C-suite executive described the struggle to simply keep the doors open. “We’re still in survival mode...we haven’t thought about permanent impacts of the pandemic. We never thought this would happen, so we’re just trying to get by.” For some, the pandemic offered a valuable lesson about how risks manifest across the organization. “COVID has taught us that we need to be more centralized and have an overarching strategy and guidance in place when it comes to risk management,” said one education sector CAE.

The complexity and dynamics of post-COVID-19 employer/employee relationships ranked high for many *OnRisk* respondents. The pandemic highlighted the importance of managing talent and culture. According to one real estate senior executive, “Our worry is about losing the culture with the new people. They never really got to experience [culture] because they go right from being hired to working from home.”

Long-term planning sessions are not top of mind for many, but respondents say they will focus more on contingency plans down the line.

“The reality is that most companies don’t have contingency plans at all. Now companies are going to have to work toward understanding contingency plans and the importance of assigning teams and positions to handle unexpected risk,” said one municipal board member.

## SENIOR EXECUTIVES AND BOARDS DESIRE BROADER SCOPE FOR INTERNAL AUDIT SERVICES

**For many organizations,** the COVID-19 experience raised awareness of not just the value of risk management alignment among key players, but also of the potential to leverage risk assurance beyond financial and compliance risks. *OnRisk* respondents expressed growing interest in expanded assurance over operational and enterprise risk, as well as the need to proactively address risks. These developments point to opportunities to leverage internal audit services even more, particularly in highly relevant risk areas such as Cybersecurity, Talent Management, and Organizational Governance. Overall, respondents feel that their current assurance services are adequate but suggest some improvements in assurance reporting.

“There was a time where we were misaligned because the auditor was focused on financial risks and not enterprise risk. An organization needs to cover both.”

– C-suite, Healthcare

As understanding and appreciation of enterprise risk management grows, so do demands on internal audit to expand its scope, identify shortfalls in risk coverage, monitor emerging risks, report clearly and concisely to stakeholders, and employ greater use of technology to provide robust risk management assurance.

One retail industry board member said it's time to broaden how internal audit is viewed within organizations. "Some people think that internal audit is too reactive and just dependent on the current needs at the moment. I think it's good to have internal audit thinking about the process, getting ahead, and identifying gaps."

A technology C-suite executive called on internal audit to expand its services to cover emerging risk areas. "Currently, our internal audit doesn't hit on some of these risks like environmental sustainability and change in regulatory environment."

Not all respondents feel internal audit is critical to adequate risk management assurance. According to one information technology C-suite executive, "We don't have internal audit, but we have external audit, and I believe it is adequate for what we need." While some organizations rely exclusively on external audit for risk management assurance, there are inherent risks in this myopic approach.

Relying on risk management assurance from external audit, which historically primarily focuses on financial reporting and compliance, is in itself risky. One technology C-suite executive articulated a more sophisticated approach to risk management, which adds needed perspective:

"We have a formal ERM process, with a person that leads annual reviews for the entire organization. Risks get rated, gaps get identified, and then the likelihood and significance as well as tolerance is determined. Two hundred risks are assessed and grouped together in different categories. I think because we have this process and our audit function is so tuned-in to risk, we have sufficient assurance."

*OnRisk* respondents said they want to see more consistency in assurance reporting, as well as better ways to communicate findings, including more data and analysis and tailored detail based on audience. One financial industry board member stressed the need to effectively present relevant and actionable risk information, "Some risk reports are maybe too detailed, which makes it difficult for extracting insights. Detail is good, but there should be summaries of relevant info for stakeholders, board members, etc."

Additionally, internal audit must demonstrate its ability to execute and add value during crises. According to one manufacturing C-suite executive, "I think of the fire drill analogy. It's easy to walk out calmly, single file, when you know there's no fire. Would we behave exactly as we did in real life?"

**CAE respondents to the OnRisk survey recognize the opportunity and need for internal audit to improve:**

*"You cannot do things alone...you have to have partnerships, that is how everybody succeeds. Rather than reporting and managing in silos, you should be consistent across the organization."*

–CAE, Government

*"We need to determine key risk indicators, measure those, reflect, re-address, re-report...it's a cycle."*

– CAE, Technology

*"There's always room for improvement in building more data analytics and assessing risk with more factual data."*

– CAE, Finance

# INSIGHTS AND ACTIONS – BOARD

---

**The wisdom of board members expanding their personal knowledge** of risks beyond financial and compliance issues has never been more evident. Swift technological changes, disruptive innovation, dynamics of organizational governance, the pandemic, and its resulting economic and political shocks provide ample impetus for board members to expand how they view their risk management role.

**In the coming year, boards should:**

**IMPROVE THEIR KNOWLEDGE OF ECONOMIC AND POLITICAL VOLATILITY.** As noted earlier, this risk area could have profound long-term impacts that could reshape how business is done. (See “Risks to pay attention to going forward – Economic and Political Volatility” on page 12).

- *Board members should develop an understanding of how volatility in both the economy and politics could impact how their organizations operate.*
- *Boards should consider directing executive management to include volatility scenarios in crisis management plans and test such scenarios and responses.*

**PUSH EXECUTIVE MANAGEMENT AND INTERNAL AUDIT ON ESG RISK MANAGEMENT.** Organizations should prepare for enhanced regulatory requirements and/or investor expectations on ESG reporting. The U.S. Securities and Exchange Commission and other regulators have clearly signaled interest in greater regulation in this area. Beyond ESG reporting, boards should push for an enterprisewide approach to managing ESG risks.

- *Request an ESG risk assessment for the organization.*
- *Ask executive management what frameworks are used to determine adequacy of the organization’s ESG reporting.*
- *Ask internal audit to perform assurance or advisory services such as those relating to assessing the design and operating effectiveness of supporting ESG controls.*

**PUSH FOR MORE INFORMATION ABOUT CULTURE AND TALENT MANAGEMENT.**

- *Consider asking for an independent assessment of the organizational culture.*
- *Demand that executive management keep the board apprised of relevant talent management decisions and changes resulting from the pandemic.*

**EMPHASIZE THE IMPORTANCE OF ORGANIZATIONAL GOVERNANCE.**

- *Continually and consistently emphasize the importance of risk alignment among key risk management players.*
  - *Reject siloed or decentralized approaches to risk management.*
  - *Promote internal audit’s role in providing independent assurance over this risk area.*
-



# INSIGHTS AND ACTIONS – C-SUITE

---

**Executive management faces a myriad of risk management challenges** complicated by the 18-month battle against COVID-19. From business continuity and crisis management to long-term implications on talent management and culture, the impacts of the pandemic will have long, lingering effects on risks and risk management.

**In the coming year, executive management should:**

**BEEF UP ITS KNOWLEDGE OF ECONOMIC AND POLITICAL VOLATILITY.** As noted earlier, this risk area could have profound long-term impacts that could reshape how business is done. (See “Risks to pay attention to going forward – Economic and Political Volatility” on page 12).

## **BUILD AND PLAN TO MATURE PROCESSES AND CONTROLS AROUND ESG REPORTING.**

- *Leverage internal audit’s understanding of enterprise risk management and proven risk frameworks to help build effective ESG internal controls.*
- *Don’t wait for external auditors to give guidance or wait for regulators to establish rules.*
- *Direct internal audit to provide assurance on the effectiveness of existing ESG controls, particularly as they relate to ESG reporting.*

## **PROACTIVELY EDUCATE BOARDS ON TALENT MANAGEMENT AND CULTURE.**

- *Carefully implement and measure relevant talent management decisions, such as work arrangement preferences, and their effect on employee morale, productivity, and retention efforts.*
  - *Obtain internal audit’s input on return-to-workplace plans and related range of risks, including impact to culture.*
-

# INSIGHTS AND ACTIONS – CAEs

---

**In the midst of one of the most volatile and dynamic periods in a century,** stakeholders are signaling the need for greater assurance on risk management. Internal audit must respond.

In the coming year, CAEs should:

## **ANTICIPATE EMERGING ESG REPORTING REQUIREMENTS.**

- *Get ahead of any new requirements by understanding processes and controls in their own organization.*
- *Advocate for adoption of established sustainability frameworks.*
- *Leverage COSO's Internal Control – Integrated Framework to begin evaluation of controls around non-financial reporting.*

## **IMPROVE THEIR KNOWLEDGE OF ORGANIZATIONAL RISK AREAS WITH HIGH RELEVANCE-CAPABILITY GAPS.**

- *Identify any risk on the OnRisk list or company list where personal knowledge falls below a HIGH rating.*

## **ACT AS A CONDUIT BETWEEN BOARD AND EXECUTIVE MANAGEMENT WHEREVER MISALIGNMENT EXISTS.**

- *Perform organizational risk analysis, leveraging the OnRisk methodology.*
- *Determine alignment on risk areas that are most relevant for the organization.*
- *Concisely share relevant highlights from OnRisk 2022 with the board and executive management to foster dialogue on how the examined risks relate to their organization.*

## **SUPPORT GREATER FOCUS ON CULTURE AND TALENT MANAGEMENT RISKS.**

- *Be cognizant of potential misalignment as the organization transitions to a post-pandemic world.*
  - *Provide assurance or advisory services related to Culture or Talent Management. For example, support board or executive management in the analysis of data resulting from employee surveys, exit interviews, or diversity and inclusion initiatives.*
-

# METHODOLOGY

## Qualitative surveys measure organization alignment

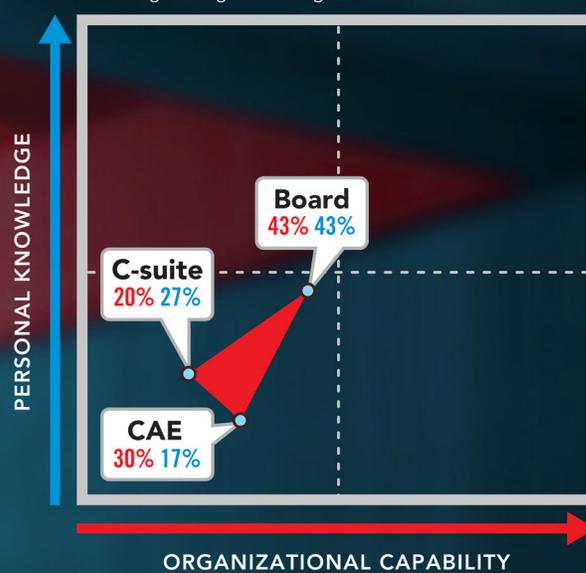
The *OnRisk 2022* report continues The IIA's groundbreaking approach in collecting stakeholder perspectives on risk and risk management in support of good governance and organizational success. The qualitative research provides a robust look at the top risks facing organizations in 2022. The report presents both objective data analysis and subjective insights based on responses from risk management leaders.

The qualitative survey is based on a total of 90 in-depth interviews with professionals in North American (U.S. and Canada) boardrooms, C-suites, and internal audit functions. The respondents came from 90 different organizations. As part of the interviews, respondents were asked to evaluate 12 key risks on three scales: Their personal awareness and knowledge of each risk, their perception of their organization's capability to address each risk, and their views of the relevance of each risk to their organization. The ratings were based on a seven-point scale, with "Not at all knowledgeable," "Extremely incapable" and "Not at all relevant" being the lowest ratings (1) and "Extremely knowledgeable," "Extremely capable" and "Extremely relevant" being the highest ratings (7).

The combined responses for the knowledge and capability ratings were then used to plot the position of each respondent group for each risk, where the X axis delineates perceived organizational capability, and the Y axis delineates personal knowledge of the risk (Figure 5). The triangle created by connecting each plot point offers a graphical depiction of alignment for each risk.

Figure 5:  
KNOWLEDGE AND CAPABILITY ALIGNMENT

Percentage who gave a rating of 6 or 7 on a scale 1 to 7



# HOW TO USE THIS REPORT

## Explanation of graphics

Based on in-depth interviews with 90 professionals, the personal knowledge and organizational capabilities of each of the three respondent groups were measured and plotted for each risk. The simple quadrant mapping provides an effective and consistent tool to reflect those views (Figure 6).

The four quadrants of the graph correspond to the magnitude of each of the two measures. For example, responses with a high average in knowledge and capability would be plotted in the top right quadrant. Conversely, responses with a low average for knowledge and capability would be plotted in the lower left quadrant. As described earlier, the averages are determined based on the percentage of respondents who provided a top 2 answer for each rating. (See “The OnRisk Approach” on page 4).

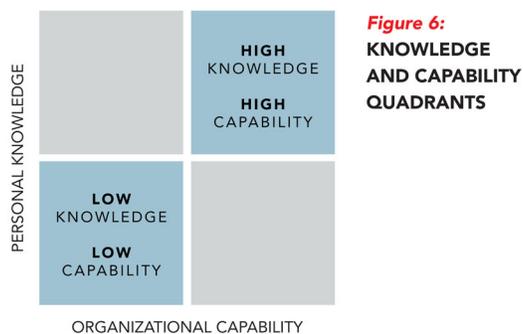


Figure 6:  
KNOWLEDGE  
AND CAPABILITY  
QUADRANTS

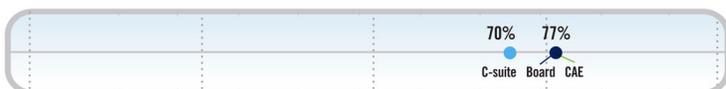
## Position plotting

Positions for each of the three respondent groups are plotted on the quadrant map not only to identify the relative knowledge and capability on each risk, but also to graphically illustrate any misalignment among the groups that may exist. The resulting triangles — referred to simply as alignment triangles in this report — provide a strong indicator of how well a risk is understood and managed. The size, shape, and location of each triangle also provides insights on what is driving any misalignment (See related sidebar).

## Risk Relevance graphic

Each respondent group’s rating on risk relevance is plotted on a single axis, providing a clear depiction of variations in the risk relevance rankings by board members, C-suite, and CAEs (Figure 7).

Figure 7: RISK RELEVANCE RATING Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



## Alignment Triangles: What do they mean?

The alignment triangles created by plotting each respondent group’s perspectives on each risk offer insights into how the risk is currently being managed. The shape of each triangle can provide valuable information, as well.



### SHORT AND NARROW

Triangles with this basic shape suggest strong alignment on what each group knows about a risk, but significant disagreement by one respondent group about the organization’s capability for addressing the risk.

### TALL AND NARROW

Conversely, triangles with this basic shape suggest significant range of knowledge among respondent groups, but strong alignment on their views on organizational capability.



### SHORT AND BROAD

This basic shape suggests disagreement by more than one respondent group, with the most significant disagreement relating to the organization’s capability to address the risk.



### TALL AND BROAD

This basic shape suggests misalignment by more than one respondent group, with significant disagreement on both knowledge and capability.



### SMALL AND SYMMETRICAL

This shape suggests strong alignment of all three respondent groups on knowledge and capability. Depending on the location of the triangle, this could reflect a risk that is well understood and managed (top right quadrant) or one that is not well understood or managed (lower left quadrant).

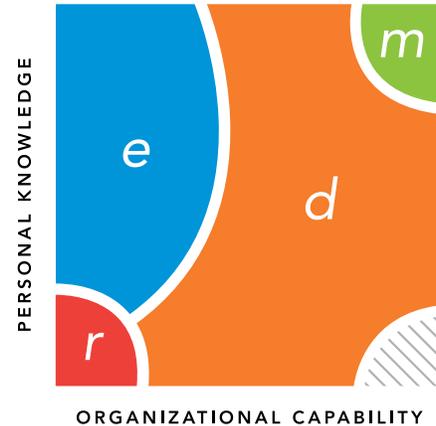


# RISK STAGES MODEL

In today's dynamic, technology-driven world, risks can emerge and mature, sometimes at breakneck speeds. The risks discussed in this report are grouped into one of four stages — Recognize, Explore, Develop, or Maintain — as they relate to the potential impact on organizations and what actions organizations should be taking to address them. The Risk Stages Model (Figure 8) reflects how risk management evolves within the organization on the same scale as the risk rankings — Personal Knowledge and Organizational Capability.

Additionally, the relevance of each risk should be understood as unique to each organization. Where each risk ranks in relevance depends on various factors, including the organization's size, industry, and type, as well as competition, maturity, position in the marketplace, supply chain, liquidity, and others. As noted earlier, there are likely risks not included in this analysis that have particular relevance to some organizations depending on their specific circumstances. Because of this unique aspect, risk relevance is not depicted in the Stages of Risk.

Figure 8:  
RISK STAGES MODEL

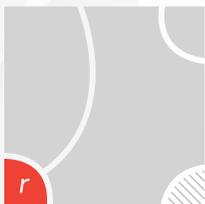


## Stages of Risk Explanation

### RECOGNIZE

A risk is perceived as emerging and knowledge of the risk among stakeholders is low. Risk response strategies are not implemented or are not assumed to be effectively designed given the low understanding of the underlying risk. Monitoring processes have not been contemplated. Inherent risk levels are not well understood.

Personal Knowledge - Low  
Organizational Capability - Low



### EXPLORE

Knowledge of the risk is growing among some stakeholders, but not by all. The risk may be perceived as emerging or dynamic. Risk response strategies have been contemplated, but not fully implemented. Monitoring processes have not been contemplated or are not implemented. Inherent risk levels are generally understood.

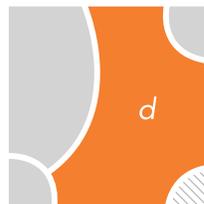
Personal Knowledge - Mid to High  
Organizational Capability - Low



### DEVELOP

Risk knowledge is high, at least with executive management teams. Risk response strategies may be developed or in process of being implemented. Monitoring processes may be in contemplation but are not likely to have been fully implemented. Residual risk is generally understood.

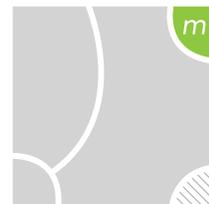
Personal Knowledge - Mid to High  
Organizational Capability - Low to High



### MAINTAIN

Risk is well understood by all relevant stakeholders and is not perceived to be changing significantly. Risk response strategies have been developed and implemented consistent with the perceived relevance of the risk. Monitoring processes are utilized to ensure risk response strategies are operating effectively as designed. Residual risk levels are understood and believed to be at an acceptable level for the organization.

Personal Knowledge - High  
Organizational Capability - High





The background features several large, textured, rectangular blocks in shades of blue, green, and yellow, arranged in a 3D perspective. A network of white lines with small red and white nodes is overlaid on the scene, particularly on the right side. The overall aesthetic is modern and digital.

# THE

# RISKS

**This section examines key observations** related to individual risks. Each risk page provides a risk definition and brief overview based on the qualitative interviews; maps alignment among key risk management players on personal knowledge, organizational capability, and relevance; shares insightful quotes from interviewees on the risk; and identifies changes in the developmental stages of each risk from the previous year, where applicable.



# THE RISKS

## CYBERSECURITY

### Definition:

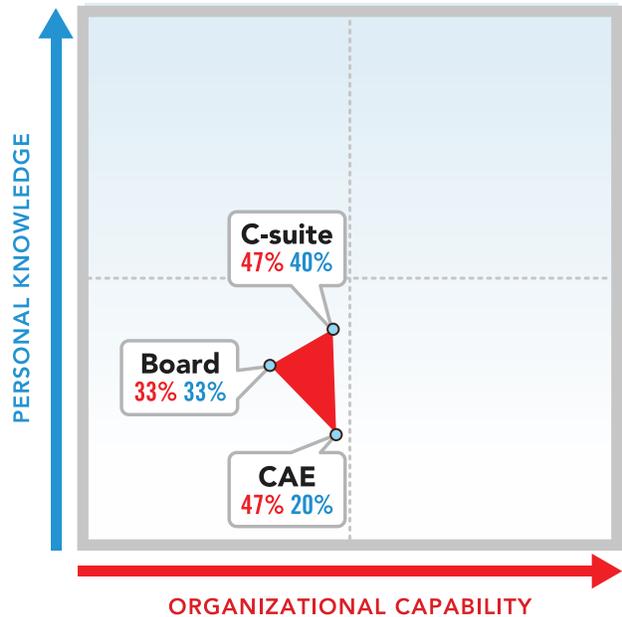
The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

### Analysis:

Nearly every member of executive management sees Cybersecurity as being highly relevant to their organization. However, personal knowledge of this highly impactful risk remains particularly low amongst all players, particularly CAEs. This low level of knowledge likely stems from the ever-evolving nature of cyber threats. Overall, a low percentage of respondents across all groups rated the capability of their organizations to manage Cybersecurity as high. In particular, few board members perceive their organization as being highly capable of managing Cybersecurity.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



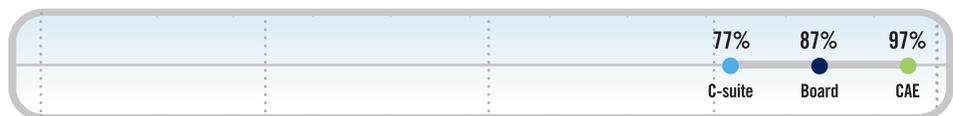
### Quotes:

"Cybersecurity risk is an ever-evolving risk. The architecture and planning processes that have been used to deal with [cybersecurity] have become more complex as technology has become more prevalent." –Board, Finance

"As we have witnessed with the pipeline hack this year, these cybersecurity attacks can have a huge trickle-down effect. All industries are susceptible to cybersecurity risk to some extent." –Board, Manufacturing

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Cybersecurity



# THE RISKS

# TALENT MANAGEMENT

## Definition:

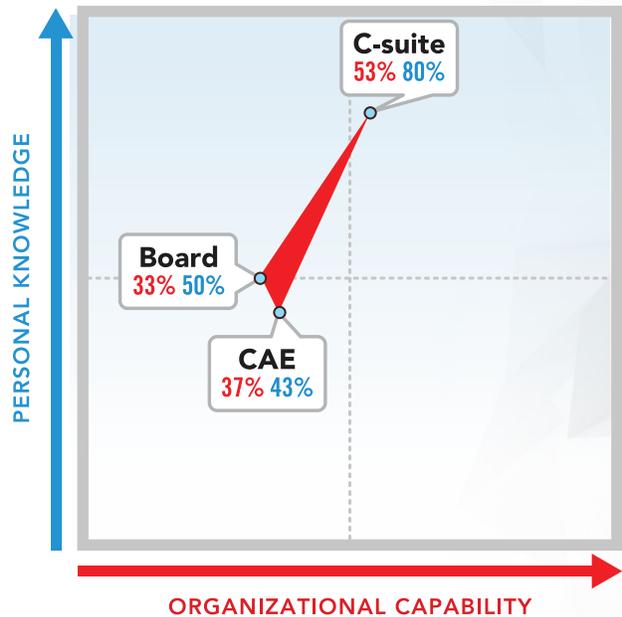
The increased need for and acceptance of remote operations, including working from home, as well as continued dynamic labor conditions are redefining how work gets done. This risk examines the challenges organizations face in identifying, acquiring, upskilling, and retaining the right talent to achieve their objectives.

## Analysis:

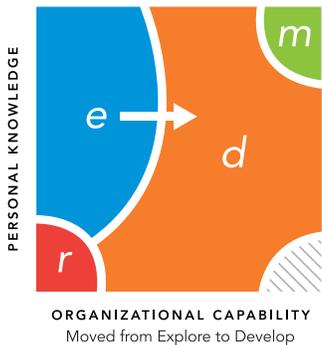
Despite all key management players seeing Talent Management as one of the most relevant risks to their organizations, perceptions of both personal knowledge and organizational capability remain relatively low for board members and CAEs. Senior executive perceptions of their personal knowledge and their organizations' capabilities in this space are much higher.

## KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



## RISK STAGE



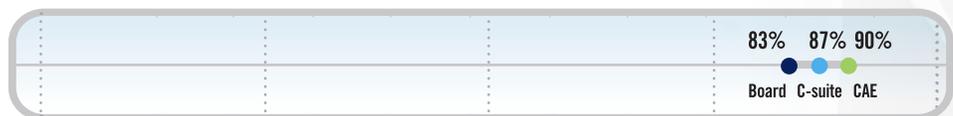
## Quotes:

"Companies are working so hard to survive...all strategies are out the window. When you don't get to see employees face-to-face, it's challenging."  
-Board, Government

"Hiring in this remote environment has allowed us to consider hiring without a geographic limitation. The question we are now asking ourselves is; do we hire a higher quality candidate to work fully remote, or do we hire a lesser candidate who is able to come into the office?" -CAE, Automotive

## RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
- Talent Management



# THE RISKS

## ORGANIZATIONAL GOVERNANCE

### Definition:

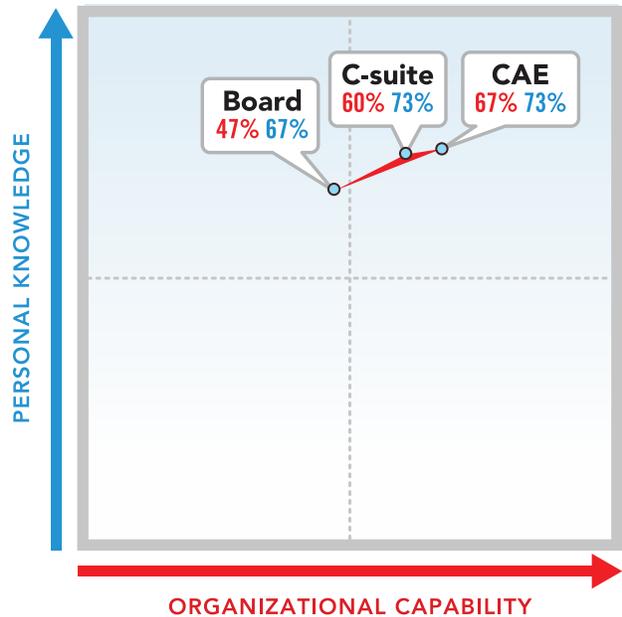
**Governance encompasses all aspects** of how an organization is directed and managed and the system of rules, practices, processes, and controls by which it operates. This risk examines whether organizations' governance assists or hinders achievement of objectives.

### Analysis:

**Personal knowledge** is high across all three risk management players of this relatively mature risk, which is widely regarded as highly relevant. However, significant misalignment exists on organizational capability to manage this important component of ESG. Fewer board members than senior executives rated their organizations as having high organizational capability for this risk area.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE

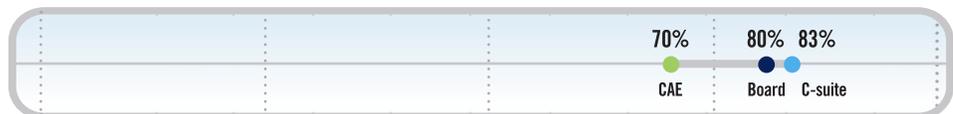


### Quotes:

- "How you plan for all of the other risks can be [attributed] to organizational governance... it's extremely important and covers everything." –C-suite, Manufacturing
- "For a lot of public companies, capability could be higher. Just look at some of the issues that arise...if everyone was really good at it, we wouldn't be seeing so much breakdown in the structures at public companies." –Board, Finance

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– **Organizational Governance**



# THE RISKS

## DATA PRIVACY

### Definition:

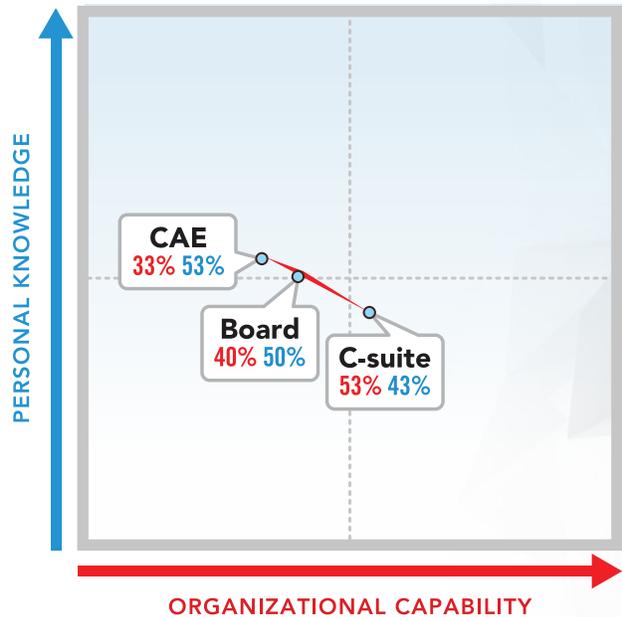
The growing list of regulations from jurisdictions around the world is making Data Privacy increasingly complex and dynamic. This risk examines how organizations protect sensitive data in their care and ensure compliance to all applicable laws and regulations.

### Analysis:

Despite having lower personal knowledge and lower perceptions of organizational relevance of this increasingly regulated risk, members of the C-suite have a higher perception of organizational capability than do either board members or CAEs.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



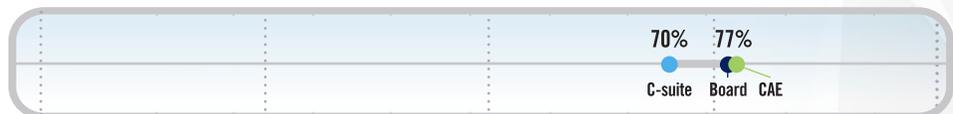
### Quotes:

"It's critical to have procedures in place to analyze, collect, and store data that are common practices throughout the organization." –CAE, Government

"I hear a ton about data privacy compared to 10 years ago, and I think it will grow in importance." –C-suite, Healthcare

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Data Privacy





# THE RISKS

## CULTURE

### Definition:

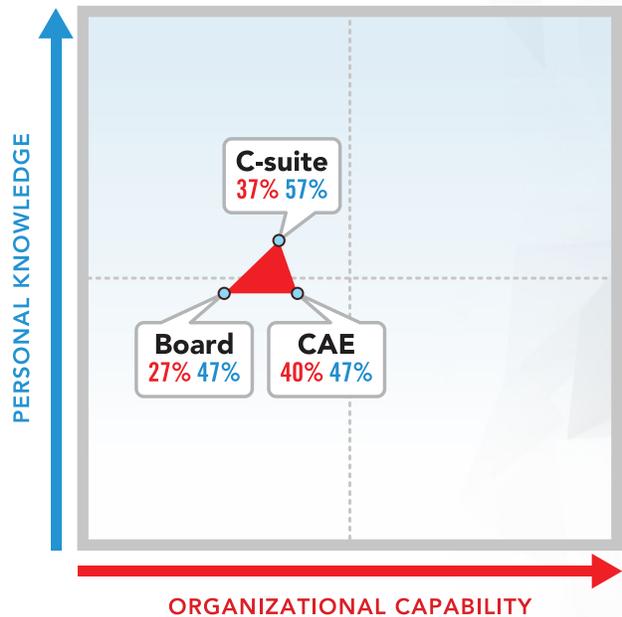
With an increasing percentage of professional employees working remotely full or part-time, organizations are challenged to maintain, enhance, or control their organizational culture. This risk examines whether organizations understand, monitor, and manage the tone, incentives, and actions that drive the desired behavior.

### Analysis:

There is strong alignment across all key risk management players regarding the relevance of Culture to organizational success. However, a gap exists between the number of board members who have high personal knowledge of this risk and senior executives who do. Similarly, fewer board members perceive their organizations as having a high capability to manage this risk, which is increasingly important to organizations as they emerge from the global pandemic.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



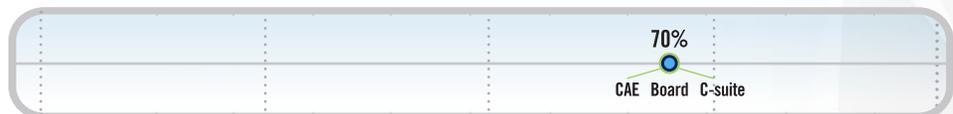
### Quotes:

"We all 'live' culture, but understanding how to manage it and change it is a different beast altogether." –CAE, Finance

"Our worry is about losing the culture with the new people. They never really got to experience [culture] because they go right from being hired to working from home." –C-suite, Real Estate

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Culture



# THE RISKS

## ECONOMIC AND POLITICAL VOLATILITY

### Definition:

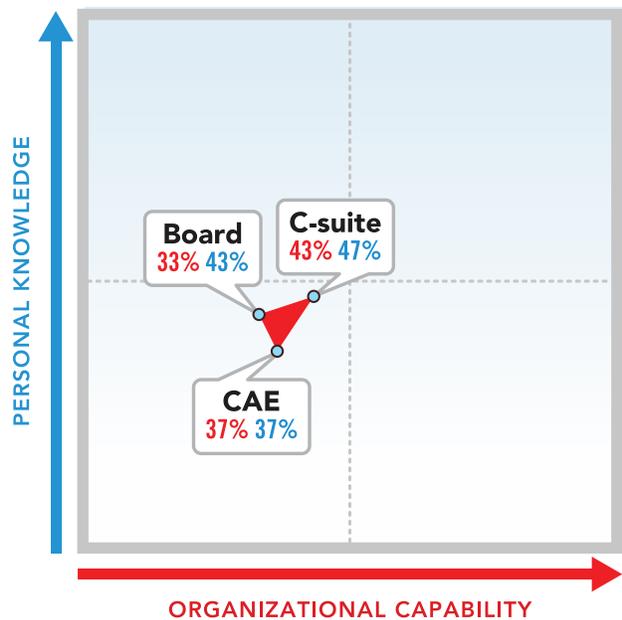
The ongoing impacts of the pandemic combined with the normal dynamics of macroeconomic cycles have the potential to create volatility in the markets in which organizations operate. This risk examines the challenges and uncertainties organizations face in a dynamic and potentially volatile economic and political environment.

### Analysis:

Overall, there is fairly strong alignment among executive management, board members, and chief audit executives across risk relevance, personal knowledge, and organizational capability. However, while more than two-thirds of all respondents saw the potential effects resulting from Economic and Political Volatility as having a high impact on their organizations, personal knowledge surrounding this risk and perceptions of organizational capability remain relatively low.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE

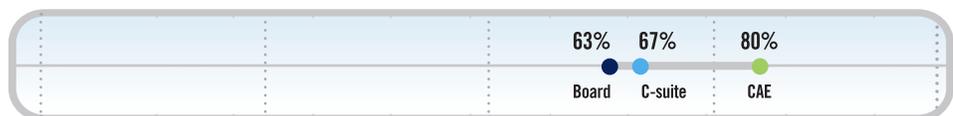


### Quote:

"Things were a breeze until 2008-2009. Now 2020-2021 into 2022, we're expecting a lot of volatility...I don't have strong feelings about where the economy is going, but we're planning more now for major impacts like product shortages, delays, disruptions like that." –C-suite, Finance

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– *Economical and Political Volatility*



## CHANGE IN REGULATORY ENVIRONMENT

### Definition:

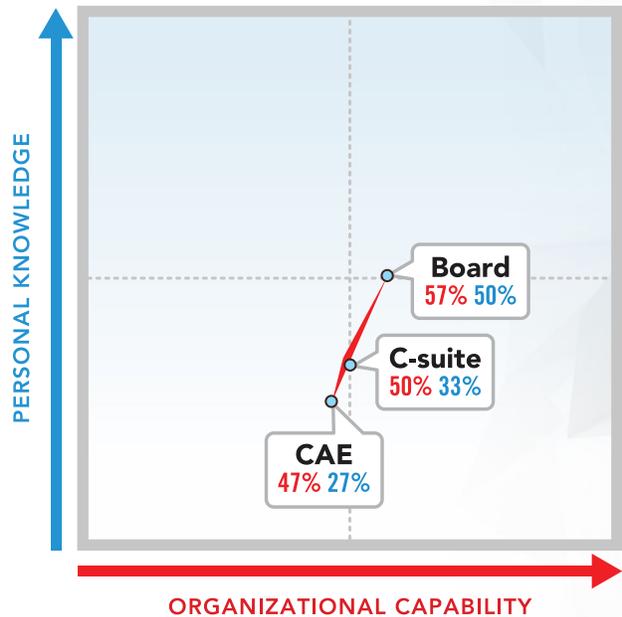
**Fundamental changes** in government appetite for regulation can have a significant impact on organizations, including those not considered heavily regulated. This risk examines the challenges organizations face in a dynamic and ambiguous regulatory environment.

### Analysis:

**Despite general alignment** on the increasing risk relevance of a changing regulatory environment, personal knowledge related to this risk is low, particularly for chief audit executives and C-suite. While personal knowledge is higher for this risk among board members, it is still lower than several other risks. Board members are somewhat more confident in the ability of their organizations to manage this important risk.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



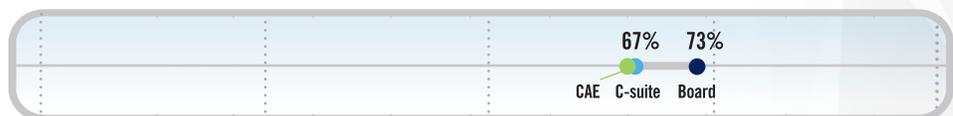
### Quotes:

"This could be a big issue for us and there is a real risk here. It is important for folks to keep their eyes on changing regulations." –CAE, Finance

"A lot of companies are reluctant to take a step forward unless forced to." –C-suite, Healthcare

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Change in Regulatory Environment



## SUPPLIER AND VENDOR MANAGEMENT

### Definition:

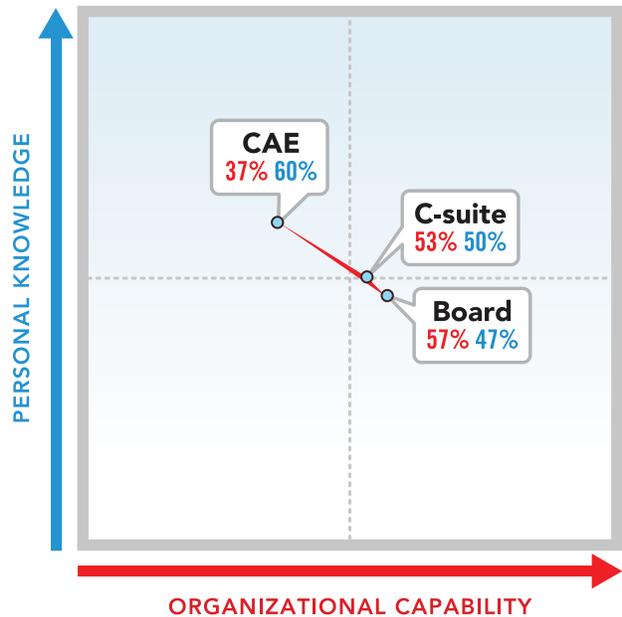
For an organization to be successful, it has to maintain healthy and fruitful relationships with its external business partners and vendors. This risk examines organizations' abilities to select and monitor third-party relationships.

### Analysis:

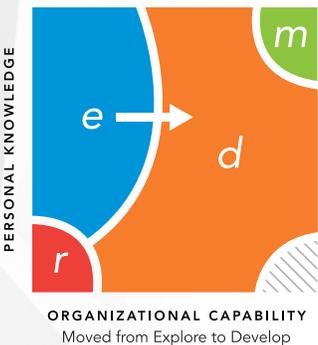
While more CAEs have high personal knowledge of this critical risk in an increasingly interconnected business environment, fewer perceive their organizations as having a high capability to manage this risk. This gap between CAEs and their stakeholders may be driven by a higher percentage of CAEs viewing this risk as being highly relevant to their organizations, likely stemming from publicly reported cyber threats, compliance-related issues, and other disruptive events arising from third-party relationships.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



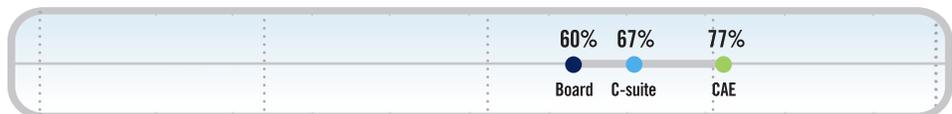
### Quotes:

"The challenge is how do we keep this relationship with these long-time vendors, and at the same time how do we go out and find what we need if that vendor cannot provide it." –C-suite, Manufacturing

"Our organization has really strong relationships...but I gave it a lower capability score because data privacy, protection, cybersecurity...those things are harder to manage with our suppliers." –CAE, Technology

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Supplier and Vendor Management



## DISRUPTIVE INNOVATION

### Definition:

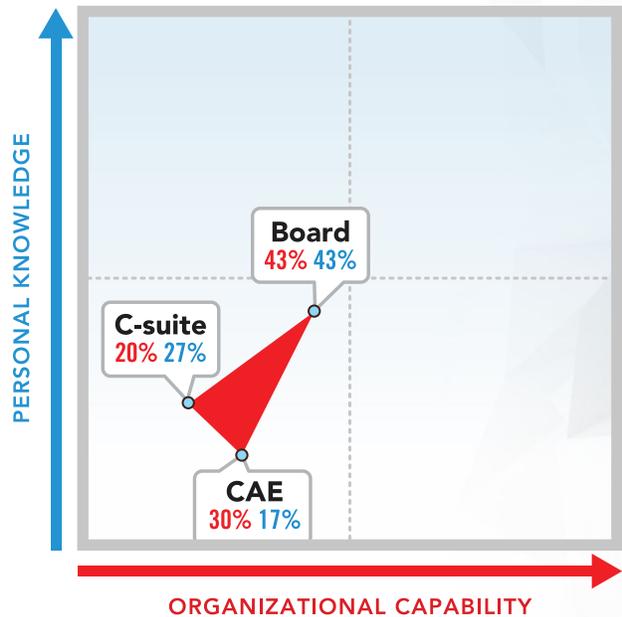
We are in an era of innovative business models, fueled by disruptive technologies. This risk examines whether organizations are prepared to adapt to and/or capitalize on disruption.

### Analysis:

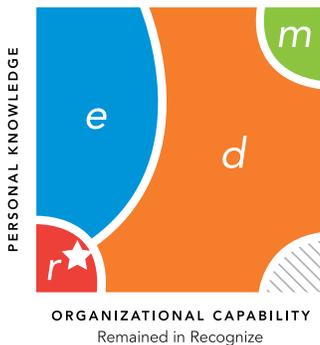
There is a fairly wide gap between the percentage of board members who see this risk as highly relevant compared to C-suite executives who do. Further, more board members perceive their personal knowledge of this very important risk as being high. However, board members may be overconfident in organizations' capability to manage Disruptive Innovation as more board members see their organizations as having high capability to manage this risk than do members of the C-suite.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



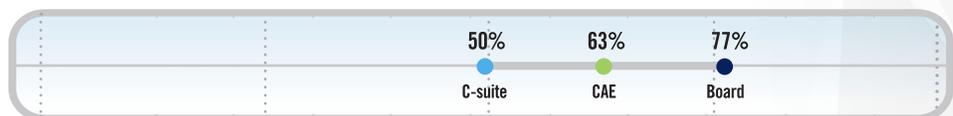
### Quotes:

"It's a matter of awareness and research...some [innovations] come and go but others hang around, like cryptocurrency." –C-suite, Nonprofit

"We're not innovative, change is very slow to happen. Everything is about bandaging... a preparedness and ability to adapt is not there." –Board, Healthcare

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Disruptive Innovation



# THE RISKS

## SOCIAL SUSTAINABILITY

### Definition:

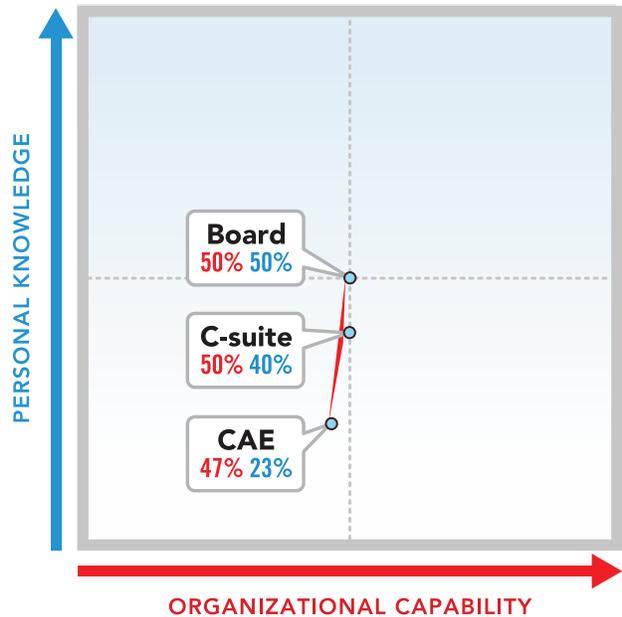
**Increasingly**, there is a recognition that organizations have significant influence on individuals who they employ, who work in their value chain, who consume their products and services, and who live in their communities. This risk examines the ability of organizations to understand and manage the direct and indirect impacts their actions have on individuals and communities.

### Analysis:

**Among the key risk management players**, there is very strong alignment on the risk relevance and perception of organizational capability for this fast-emerging risk that touches all industries. However, the CAE group significantly lags behind its stakeholder groups related to personal knowledge of this risk.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



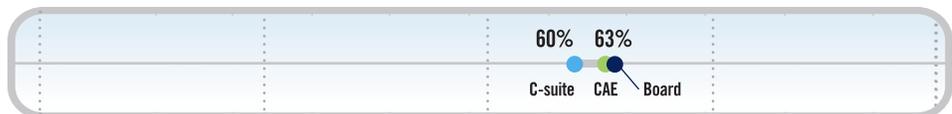
### Quote:

*"Sustainability is going to be an absolute imperative in order to preserve, maintain, and grow wealth. This is like any other investment in business. These investments need to be made in order to protect and sustain the value that's being created."*

–Board, Finance

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Social Sustainability



## SUPPLY CHAIN DISRUPTION

### Definition:

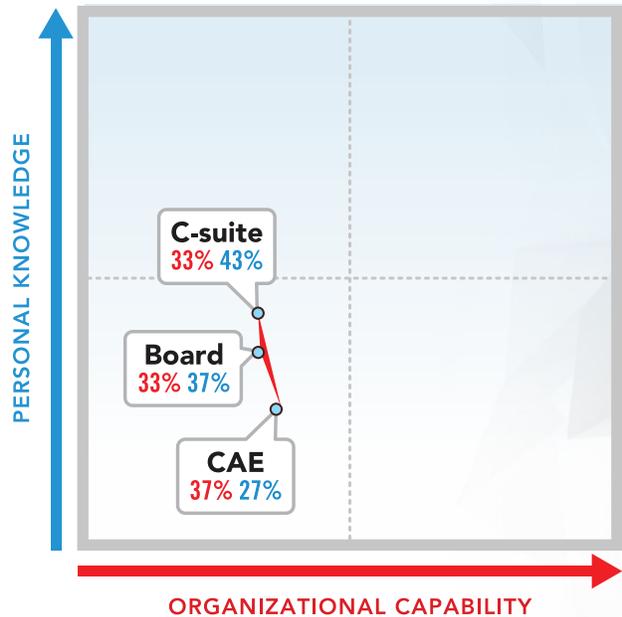
The disruption to business-as-usual operations globally, rooted in the global pandemic, has highlighted the need for resilience in supply chains in support of organizations' achievement of strategic objectives. This risk examines whether organizations have built in the flexibility to adapt to current and future supply chain disruptions.

### Analysis:

There is strong alignment among board members and senior executives with regard to the risk relevance of Supply Chain Disruption, with slightly more than half of these stakeholders seeing it as a highly relevant risk to their organizations. The CAE group lags behind in personal knowledge of this increasingly important risk in the global economy, which may be a result of fewer CAEs seeing this risk as highly relevant to their organizations.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



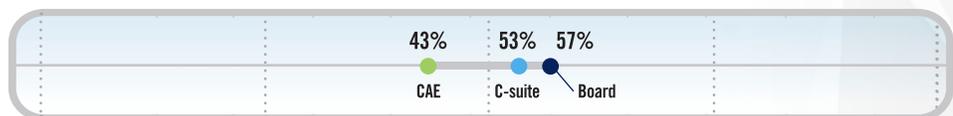
### Quotes:

"Borders closing down, and things like the Suez Canal getting plugged up have made us more in tune with supply chain issues."  
–CAE, Finance

"It used to just be what we thought about when we pulled up to the gas pump... now it's of importance across many industries."  
–Board, Finance

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Supply Chain Disruption



# THE RISKS

## ENVIRONMENTAL SUSTAINABILITY

### Definition:

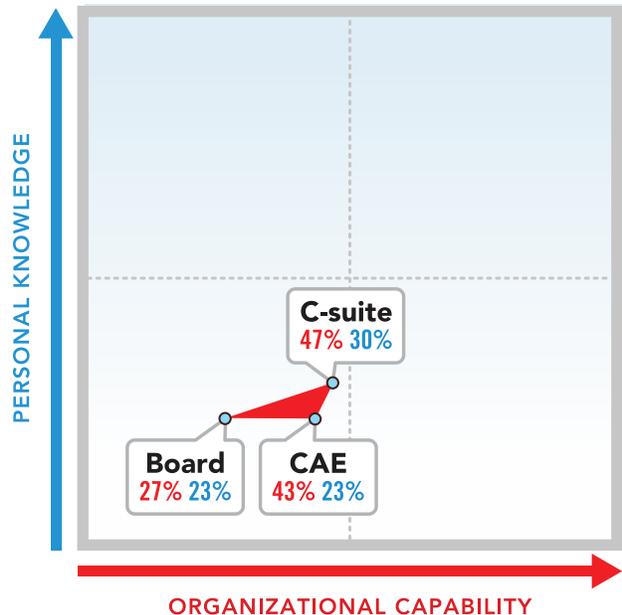
**Organizations are facing increased pressure** from stakeholders, including shareholders, regulators, customers, and employees, to evaluate and disclose how they are impacting the environment in which they operate. This risk examines the ability of organizations to reliably measure, evaluate, and accurately report on their environmental impacts.

### Analysis:

**While there is fairly strong alignment in this area,** relatively few respondents, particularly senior executives, see this quickly emerging risk as one that could be highly relevant to their organizations. Personal knowledge across all groups was also quite low. Fewer board members believe that their organizations have high capability to manage Environmental Sustainability risks.

### KNOWLEDGE AND CAPABILITY

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7



### RISK STAGE



### Quotes:

*“There is the issue of measurement for every organization. There’s a lack of standardized measurement and reporting in this area which creates confusion.”*  
–CAE, Healthcare

*“Most organizations want to have good environmental sustainability policies, procedures, and programs, but it is not always front and center when dealing with all these other risks.”* –Board, Healthcare

### RISK RELEVANCE

Percentage who gave a rating of 6 or 7 on a scale of 1 to 7  
– Environmental Sustainability







---

**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 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit [www.globaliia.org](http://www.globaliia.org).

**Disclaimer**

The IIA publishes this document for informational and educational purposes. This 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 seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

**Copyright**

Copyright © 2021 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact [copyright@theiia.org](mailto:copyright@theiia.org).

**Global Headquarters**

The Institute of Internal Auditors  
1035 Greenwood Blvd., Suite 401  
Lake Mary, FL 32746, USA  
Phone: +1-407-937-1111  
Fax: +1-407-937-1101  
[www.globaliia.org](http://www.globaliia.org)



The Institute of  
Internal Auditors

---

# 2024

## RISK IN FOCUS

Hot topics  
for internal  
auditors

---

NORTH AMERICA

---

[Read more](#)



Internal Audit  
**FOUNDATION**

# ABOUT RISK IN FOCUS

**Risk in Focus provides practical, data-driven research to help internal auditors and their stakeholders understand today's risk environment and prepare audit plans for the year ahead.**

Reports are based on a worldwide survey to identify current and emerging risks for each region, followed up with roundtables and interviews to discover leading practices for internal auditors.

Each of The IIA's six regions will receive two reports:

- **Hot Topics for Internal Auditors** – Detailed reports based on the survey, roundtables, and interviews.
- **Board Briefing** – Summary reports for internal auditors to share with stakeholders.

Global Risk in Focus is a collaborative partnership facilitated by the [Internal Audit Foundation](#) with

generous support from IIA regional bodies, IIA Institutes, and corporate sponsors. 2024 marks the first year the project was conducted worldwide.

The Risk in Focus methodology was originally created in 2016 by the European Institutes Research Group (EIRG), which continues to publish it in Europe through the European Confederation of Institutes of Internal Auditing (ECIIA).

Reports are available free to the public at The IIA's [Risk in Focus resource page](#) and at the websites for IIA regional groups: [ACIIA](#) (Asia Pacific), [AFIIA](#) (Africa), [ARABCIIA](#) (Middle East), [ECIIA](#) (Europe), [FLAI](#) (Latin America).

**NORTH AMERICA REPORT SPONSOR**



# CONTENTS

<b>4</b>	Executive summary – North America	<hr/>
<b>5</b>	Methodology	<hr/>
<b>6</b>	Survey results: Global	<hr/>
<b>13</b>	Survey results: North America	<hr/>
<b>21</b>	Cybersecurity: Team building for cyber resilience	<hr/>
<b>26</b>	Human capital: Negotiating the culture clash	<hr/>
<b>31</b>	Market changes: Adding value with strategic involvement	<hr/>
<b>35</b>	Business continuity: Building resilience in complexity	<hr/>
<b>40</b>	Interconnected risks: Geopolitical uncertainty, supply chain, and regulatory change	<hr/>
<b>44</b>	Future expectations: Pressure grows from digital disruption and climate change	



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## EXECUTIVE SUMMARY – NORTH AMERICA

### Responding to rapid change with collaboration

**After an unprecedented three years of global disruption, North American organizations are seeking closer collaboration with stakeholders across their organizations to get in front of the fast-moving risk landscape. Internal audit leaders are often acting as advisors to the board and management on mission-critical projects and retooling audit methodologies to better manage the risks ahead.**

North America Risk in Focus provides insight into urgent questions facing CAEs and their boards, including:

- What are the top risks organizations face in the region? How will these develop over the next three years?
- Where are internal auditors investing the most time and effort?
- How can internal audit functions help their organizations?

Two risks dominate the risk landscape for North America in 2024 – cybersecurity and human capital, which cut across almost every aspect of an organization's operations. By 2027, CAEs expect the biggest risk to still be cybersecurity, but digital disruption will leap into second place – with climate change also seeing greatly increased risk levels.

Among survey respondents worldwide,

the three areas of highest risk were cybersecurity, human capital, and business continuity. Across regions there was remarkable consensus that digital disruption and climate change were the two areas expected to increase the most for risk level and audit effort.

The North America Risk in Focus reports describe in detail the challenges and solutions for urgent risk areas and draw on the expertise, experience, and knowledge of multiple internal audit leaders throughout the region. The featured topics for the North America reports are cybersecurity, human capital, market changes, and business continuity.

**For a summary of findings to provide to boards and stakeholders, see [North America Risk in Focus 2024 – Board Briefing](#). For reports from other regions, see the [Risk in Focus resource page](#).**

## North America Research Participation

- 442 survey responses from CAEs and directors
- Participating countries: U.S. (385), Canada (57)
- 4 roundtables with 28 participants
- 9 in-depth interviews



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## METHODOLOGY

**The Risk in Focus methodology starts with a survey of CAEs and heads of internal audit to identify current and emerging risks for each region. The top risks identified in the survey are used in follow-up roundtables and interviews with CAEs, academics, and other industry experts.**

The survey presents 16 risk categories, shown below. Respondents are asked to choose the top 5 highest for risk level and the top 5 highest for internal audit time and effort – both for now and three years in the future. In reports, the categories are referenced by their shortened names.

For the Risk in Focus 2024 project worldwide, survey responses were received from 4,207 CAEs and directors in 111 countries/territories from February 15 to July 12, 2023. Eighteen roundtables were conducted with 152 participants, followed by 40 in-depth interviews.

### Risk in Focus 2024 Risk Categories

Risk Topic	Risk Description Used in the Survey
Business continuity	Business continuity, operational resilience, crisis management, and disaster response
Climate change	Climate change, biodiversity, and environmental sustainability
Communications/reputation	Communications, reputation, and stakeholder relationships
Cybersecurity	Cybersecurity and data security
Digital disruption	Digital disruption, new technology, and AI
Financial liquidity	Financial, liquidity, and insolvency risks
Fraud	Fraud, bribery, and the criminal exploitation of disruption
Geopolitical uncertainty	Macroeconomic and geopolitical uncertainty
Governance/corporate reporting	Organizational governance and corporate reporting
Health and safety	Health, safety, and security
Human capital	Human capital, diversity, and talent management and retention
Market changes	Market changes/competition and customer behavior
Mergers and acquisitions	Mergers and acquisitions
Organizational culture	Organizational culture
Regulatory change	Change in laws and regulations
Supply chain and outsourcing	Supply chain, outsourcing, and 'nth' party risk

**111**  
countries/  
territories

**4,207**  
survey  
responses  
from CAEs

**18**  
roundtables with  
**152**  
participants

**40**  
in-depth  
interviews



## Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

# SURVEY RESULTS – GLOBAL

## Regional comparisons

The worldwide participation in the Risk in Focus survey provides a rare opportunity to compare risk and audit planning between different regions.

## How to use survey results

The Risk in Focus survey results are presented in a series of graphs that show survey responses about risk levels and audit effort – both now and three years in the future. Key findings are summarized below, but readers are encouraged to review the graphs in detail to obtain further insights.

Percentages show how many chose an audit area as one of the five highest for risk level or audit effort at their organization.

In the graphs, results for risk levels are colored blue, and results for audit effort are green; current levels are darker shades and future levels are lighter.

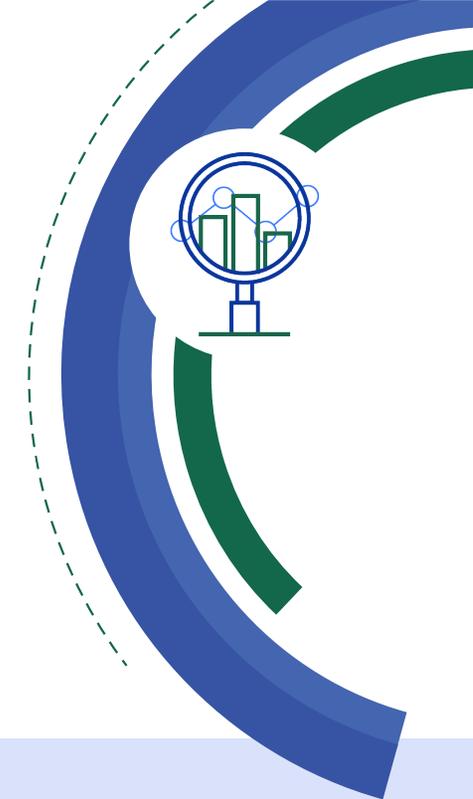
### Figure 1: Top 5 highest risks per region – Global

There is broad consensus worldwide that the three areas of highest risk for the organizations where CAEs work are:

1. Cybersecurity
2. Human capital
3. Business continuity

For most regions, regulatory change also ranks as a top 5 highest risk, with the exception of Africa and Middle East, where financial liquidity is more of a concern. Reflecting current events and future concerns, geopolitical instability topped the list for Latin America and Europe. Market changes were considered a top risk for Asia Pacific and North America, but not in other regions.

Finally, Africa was the only one with fraud as a top 5 concern, while the Middle East was unique for having governance/corporate reporting in their top 5.



## Global Survey – Responses Per Region

Africa	808
Asia Pacific	1,035
Latin America (& Caribbean)	956
Europe	799
North America	442
Middle East	167
<b>Total</b>	<b>4,207</b>



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

# SURVEY RESULTS – GLOBAL

Another way to look at the data is to consider which region had the highest risk within each audit area. For example, climate change risks were rated highest in Europe, compared to other regions. Some notable points about highest ratings per audit area include:

- North American respondents gave cybersecurity (85%) and human capital (65%) the highest risk ratings compare to other regions.
- For Europe, while cybersecurity was nearly as high as for North America (84%) the other areas of high concern were geopolitical uncertainty (43%) and climate change (31%). Europe was the only region where climate change was higher than 30%.
- Latin America shared Europe’s concern about geopolitical uncertainty (42%), but also reported high risk for regulatory change (48%) and digital disruption (38%).
- Asia Pacific was particularly concerned with business continuity (61%) and market changes (47%), compared to other regions.

- The Middle East had much higher risk levels for governance/corporate reporting (45%) than other regions and was also slightly higher for communications/reputation (28%).
- Finally, Africa had a unique mix of risks that were higher than other regions, including financial liquidity (47%), fraud (46%), and organizational culture (34%).

## Figure 2: Top 5 audit effort per region – Global

Although risk levels may vary from region to region, the areas of highest effort for internal audit are remarkably similar, generally in this order:

1. Cybersecurity
2. Governance/corporate reporting
3. Business continuity
4. Regulatory change
5. Financial liquidity
6. Fraud

The primary area of difference was for regulatory change, where audit effort percentages were notably lower for Africa (35%) and Middle East (35%) than other regions, which were at 50% or higher.

Although risk levels may vary from region to region, the areas of highest effort for internal audit are remarkably similar.

Other specific differences were:

- Asia Pacific had a lower percentage for financial liquidity (35%) than the global average (45%).
- Latin America was lower than other regions for effort toward governance/corporate reporting (46% for Latin America vs. 55% global average).
- North America was much lower than the global average for fraud effort (26% for North America vs. 42% global average).



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## SURVEY RESULTS – GLOBAL

Another way to look at the data is to consider which region had the highest audit effort within each audit area. In many audit areas, the difference in effort between regions is small. But there were some audit areas where differences were notable:

- North America was much more broadly involved in cybersecurity (84%) than other regions, with the exception of Europe (79%).
- Africa has more functions putting top 5 effort toward fraud (57%) and financial liquidity (53%) than other regions.
- Europe has almost double the percentage who say climate change is top 5 for audit effort (19%) compared to the global average (11%).

### Figure 3: Expected risk change in three years – Global

There is consensus worldwide that risk levels will rise in the next three years for digital disruption and climate change. Both areas saw increases of about 20 percentage points between current and future risk levels. Even more remarkable is the increase in ranking for climate change, which leaped from fourteenth place to fifth.

### Figure 4: Expected audit effort change in three years – Global

With risk levels expected to rise for digital disruption and climate change, so is the amount of time and effort internal audit expects to spend in these areas. The percentage expecting digital disruption to be top 5 for audit effort more than doubled - from 22% to 52%. Equally remarkable, the percentage for climate change more than tripled, from 11% to 34%.

There is consensus worldwide that risk levels will rise in the next three years for digital disruption and climate change.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

Figure 1:

## Top 5 highest risks per region – Global

Highest risks per region

There is broad consensus worldwide that the three areas of highest risk are cybersecurity, human capital, and business continuity.

### What are the top 5 risks your organization currently faces?

Audit area	Average of all regions	Asia Pacific	Latin America	Africa	North America	Middle East	Europe
Cybersecurity	73%	66%	75%	58%	85%	70%	84%
Human capital	51%	59%	44%	39%	65%	47%	50%
Business continuity	47%	61%	47%	52%	36%	53%	35%
Regulatory change	39%	35%	48%	32%	43%	33%	43%
Digital disruption	34%	30%	38%	33%	36%	32%	33%
Financial liquidity	32%	21%	33%	47%	28%	38%	26%
Market changes	32%	47%	26%	21%	41%	26%	30%
Geopolitical uncertainty	30%	28%	42%	25%	28%	16%	43%
Governance/corporate reporting	27%	24%	18%	36%	16%	45%	22%
Supply chain and outsourcing	26%	27%	16%	19%	36%	28%	30%
Organizational culture	26%	23%	26%	34%	21%	30%	20%
Fraud	24%	22%	30%	46%	9%	26%	13%
Communications/reputation	21%	18%	22%	27%	21%	28%	12%
Climate change	19%	22%	22%	19%	12%	10%	31%
Health and safety	11%	12%	8%	10%	17%	9%	13%
Mergers and acquisitions	6%	4%	3%	3%	8%	10%	8%

Note: The IIA's Risk in Focus Global Survey, n = 4,207. Percentages show who ranked the area as one of their top 5 for risk level. Dark blue shading indicates the 5 areas of highest risk for that region.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

Figure 2:

## Top 5 audit effort per region – Global

Highest effort areas per region

■ The areas of highest audit effort across regions are remarkably similar.

What are the top 5 risks on which internal audit spends the most time and effort?

Audit area	Average of all regions	Asia Pacific	Latin America	Africa	North America	Middle East	Europe
Cybersecurity	68%	66%	66%	54%	84%	61%	79%
Governance/corporate reporting	55%	54%	46%	52%	55%	64%	61%
Business continuity	54%	59%	53%	56%	53%	53%	50%
Regulatory change	46%	56%	50%	35%	53%	35%	50%
Financial liquidity	45%	35%	50%	53%	46%	44%	45%
Fraud	42%	42%	47%	57%	26%	43%	36%
Supply chain and outsourcing	34%	33%	28%	32%	38%	39%	36%
Human capital	30%	33%	28%	33%	26%	35%	26%
Organizational culture	24%	23%	29%	27%	17%	27%	21%
Digital disruption	22%	19%	24%	24%	25%	20%	21%
Communications/reputation	20%	21%	23%	25%	20%	23%	11%
Health and safety	17%	18%	12%	13%	21%	16%	19%
Market changes	16%	23%	17%	15%	14%	16%	10%
Climate change	11%	10%	8%	11%	9%	7%	19%
Geopolitical uncertainty	9%	6%	13%	12%	4%	8%	8%
Mergers and acquisitions	6%	3%	5%	2%	10%	8%	9%

Note: The IIA's Risk in Focus Global Survey, n = 4,207. Percentages show who ranked the area as one of their top 5 for audit time and effort. Dark green shading indicates the 5 highest audit effort areas for that region.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

Figure 3:

## Expected risk change in 3 years – Global

Expected risk change

Climate change risks are expected to increase dramatically from the fourteenth to fifth place.

What are the top 5 risks your organization currently faces?

What are the top 5 risks your organization will face 3 years from now?

1.	Cybersecurity	73%
2.	Human capital	51%
3.	Business continuity	47%
4.	Regulatory change	39%
5.	<b>Digital disruption</b>	<b>34%</b>
6.	Financial liquidity	32%
7.	Market changes	32%
8.	Geopolitical uncertainty	30%
9.	Governance/corporate reporting	27%
10.	Supply chain and outsourcing	26%
11.	Organizational culture	26%
12.	Fraud	24%
13.	Communications/reputation	21%
14.	<b>Climate change</b>	<b>19%</b>
15.	Health and safety	11%
16.	Mergers and acquisitions	6%

1.	Cybersecurity	67%
2.	<b>Digital disruption</b>	<b>55%</b>
3.	Human capital	46%
4.	Business continuity	41%
5.	<b>Climate change</b>	<b>39%</b>
6.	Regulatory change	39%
7.	Geopolitical uncertainty	34%
8.	Market changes	33%
9.	Supply chain and outsourcing	25%
10.	Financial liquidity	23%
11.	Organizational culture	21%
12.	Governance/corporate reporting	20%
13.	Fraud	20%
14.	Communications/reputation	15%
15.	Health and safety	11%
16.	Mergers and acquisitions	11%



Note: The IIA's Risk in Focus Global Survey, n = 4,207. Percentage who ranked the area as one of their organization's top 5 highest risks.

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



Figure 4:

## Expected audit effort change in 3 years – Global



Steep rises are expected for internal audit activity related to digital disruption and climate change.

What are the top 5 risks on which internal audit spends the most time and effort?

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?

1. Cybersecurity	68%	1. Cybersecurity	73%
2. Governance/corporate reporting	55%	<b>2. Digital disruption</b>	<b>52%</b>
3. Business continuity	54%	3. Business continuity	49%
4. Regulatory change	46%	4. Regulatory change	37%
5. Financial liquidity	45%	5. Governance/corporate reporting	36%
6. Fraud	42%	6. Human capital	35%
7. Supply chain and outsourcing	34%	<b>7. Climate change</b>	<b>34%</b>
8. Human capital	30%	8. Fraud	29%
9. Organizational culture	24%	9. Financial liquidity	28%
<b>10. Digital disruption</b>	<b>22%</b>	10. Supply chain and outsourcing	28%
11. Communications/reputation	20%	11. Organizational culture	24%
12. Health and safety	17%	12. Market changes	22%
13. Market changes	16%	13. Communications/reputation	16%
<b>14. Climate change</b>	<b>11%</b>	14. Geopolitical uncertainty	16%
15. Geopolitical uncertainty	9%	15. Health and safety	15%
16. Mergers and acquisitions	6%	16. Mergers and acquisitions	8%

Note: The IIA's Risk in Focus Global Survey, n = 4,207. Percentage who ranked the area as one of their organization's top 5 highest risks.

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

# SURVEY RESULTS – NORTH AMERICA

## How to use survey results

Key findings for North America are summarized below, but readers are encouraged to review the graphs that follow in detail to obtain further insights. Percentages show how many chose an audit area as one of the five highest for risk level or audit effort at their organization. Results for risk levels are colored blue, and results for audit effort are green; current levels are darker shades and future levels are lighter.

### Figure 5: Current risk levels vs. future risk levels – North America

- Cybersecurity and human capital dominated the risk landscape for North America for 2024.
- In the next three years, digital disruption and climate change are the risks expected to increase the most.

### Figure 6: Expected risk level change in 3 years – North America

- Digital disruption is expected to move from the sixth highest risk

to the second highest in the next three years.

- Climate-related risks climb into ninth position, up from the bottom three.

### Figure 7: Current audit effort vs. future audit effort – North America

- Overwhelmingly, CAEs chose cybersecurity as a top 5 area for internal audit effort (84%).
- Second place is held by governance/corporate reporting, but this area is expected to decrease in the future.

### Figure 8: Expected audit effort change in 3 years – North America

- Steep rises are expected for activity to deal with digital disruption and climate change.
- Increases are offset by reductions for financial liquidity and governance/corporate reporting.

### Figure 9: Current risk levels vs. current audit effort – North America

- Governance/corporate reporting is low risk for organizations (16%)

but high effort (55%) for internal audit in North America.

- Effort is low compared to risk for geopolitical uncertainty, market changes, and climate change, but these risks may be addressed through financial liquidity, business continuity, or supply chain.

### Figure 10: Future risk levels vs. future audit effort – North America

- Risk levels and effort are expected to be closely aligned in the next three years for the rising risk areas of digital disruption (56% /53%) and climate change (30%/27%).



## North America Survey Responses Per Country

United States	385
Canada	57
<b>Total</b>	<b>442</b>



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



# SURVEY RESULTS – NORTH AMERICA

## Understanding the impact of SOX in North America on survey results

To better understand audit activities in North America, it's important to recognize the effect of Sarbanes-Oxley (SOX) requirements and ERM responsibility on internal audit functions, says Richard Chambers, senior audit advisor at AuditBoard.

The Sarbanes-Oxley Act of 2002 established extensive regulatory requirements for internal controls over financial reporting for publicly traded companies in the United States. Internal audit is often tasked with the lion's share of this effort, with 67% of internal audit functions at publicly traded companies saying they have direct responsibility, according to The IIA's 2023 North American Pulse of Internal Audit survey.<sup>1</sup>

In the Risk in Focus survey, Sarbanes-Oxley activity falls under the category of organizational governance/corporate reporting. This area ranked near the bottom for risk (16% as one of their top 5), but it ranked second for audit time and effort (55% at top 5). This effort toward corporate reporting tends to draw audit time away from other areas,

increasing gaps between risk and effort in other areas.

In addition to the bandwidth challenge, Chambers noted that Sarbanes-Oxley can also create an independence challenge for internal audit. Among 2023 Pulse survey respondents, 72% of CAEs at publicly traded companies say they report administratively to the chief financial officer (CFO), who is often in charge of the SOX program.

This high level of responsibility for SOX, combined with administrative reporting to the CFO, creates a risk that CAEs are not only providing assurance for internal controls over financial reporting, but are also taking on the CFO's compliance responsibilities directly. At issue is internal audit having enough independence to provide assurance for internal controls over financial reporting, given its responsibilities and reporting line.

Finally, almost half of CAEs at publicly traded companies (46%) are also responsible for ERM, according to 2023 Pulse survey respondents. On the

## Recommended Reading

[The IIA's Three Lines Model](#)

Risk in Focus frequently refers to the influential Three Lines Model, which explains the roles of the first, second, and third lines.

[The IIA's North American Pulse of Internal Audit](#)

This annual report provides benchmarks about budgets, staff, and CAE responsibilities.

positive side, when one role is responsible for both, there may be closer alignment between risk assessment and audit activity. However, it's important for CAEs to be properly trained in ERM methodology, which places equal emphasis on opportunities and risk. Finally, if internal audit is responsible for ERM, it is preferable for a third party to provide assurance for the overall effectiveness of risk management because the internal audit function should not audit its own activity.

<sup>1</sup> For survey results cited from the Pulse of Internal Audit, see page 43 (reporting lines) and page 35 (ERM responsibility) at <https://www.theiia.org/en/resources/research-and-reports/pulse/>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

Figure 5:

## Current risk levels vs. future risk levels – North America



■ Cybersecurity and human capital dominated the risk landscape for North America for 2024.  
 ■ In the next 3 years, digital disruption and climate change are the risks expected to increase the most.

### What are the top 5 risks your organization currently faces?



### What are the top 5 risks your organization will face 3 years from now?



Note: The IIA's Risk in Focus Global Survey, North America, n = 442. Percentage who ranked the area as one of their organization's top 5 highest risks.

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

Figure 6:

## Expected risk level change in 3 years – North America

Expected risk change

- Digital disruption is expected to move from the sixth highest risk to the second highest in the next 3 years.
- Climate-related risks climb into ninth position, up from the bottom three.

What are the top 5 risks your organization currently faces?

What are the top 5 risks your organization will face 3 years from now?

1. Cybersecurity	85%	1. Cybersecurity	73%
2. Human capital	65%	2. <b>Digital disruption</b>	<b>56%</b>
3. Regulatory change	43%	3. Human capital	51%
4. Market changes	41%	4. Regulatory change	50%
5. Business continuity	36%	5. Market changes	38%
6. <b>Digital disruption</b>	<b>36%</b>	6. Business continuity	35%
7. Supply chain and outsourcing	36%	7. Supply chain and outsourcing	31%
8. Geopolitical uncertainty	28%	8. Geopolitical uncertainty	30%
9. Financial liquidity	28%	9. <b>Climate change</b>	<b>30%</b>
10. Communications/reputation	21%	10. Organizational culture	21%
11. Organizational culture	21%	11. Financial liquidity	20%
12. Health and safety	17%	12. Governance/corporate reporting	18%
13. Governance/corporate reporting	16%	13. Communications/reputation	13%
14. <b>Climate change</b>	<b>12%</b>	14. Health and safety	12%
15. Fraud	9%	15. Mergers and acquisitions	12%
16. Mergers and acquisitions	8%	16. Fraud	10%



Note: The IIA's Risk in Focus Global Survey, North America, n = 442. Percentage who ranked the area as one of their organization's top 5 highest risks.

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



Figure 7:

## Current audit effort vs. future audit effort – North America



Overwhelmingly, CAEs chose cybersecurity as a top 5 area for internal audit effort (84%).  
Second place is held by governance/corporate reporting, but this area is expected to decrease in the future.

What are the top 5 risks on which audit spends the most time and effort?

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?



Note: The IIA's Risk in Focus Global Survey, North America, n = 442. Percentage who ranked the area as one of their top 5 for audit time and effort.

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

Figure 8:

## Expected audit effort change in 3 years – North America

Expected effort change

- Steep rises are expected for activity to deal with digital disruption and climate change.
- Increases are offset by reductions for financial liquidity and governance/corporate reporting.

What are the top 5 risks on which internal audit spends the most time and effort?

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?

1. Cybersecurity	84%	1. Cybersecurity	80%
2. Governance/corporate reporting	55%	2. <b>Digital disruption</b>	<b>53%</b>
3. Business continuity	53%	3. Regulatory change	49%
4. Regulatory change	53%	4. Business continuity	46%
5. Financial liquidity	46%	5. Governance/corporate reporting	38%
6. Supply chain and outsourcing	38%	6. Supply chain and outsourcing	36%
7. Fraud	26%	7. Human capital	32%
8. Human capital	26%	8. Financial liquidity	29%
9. <b>Digital disruption</b>	<b>25%</b>	9. <b>Climate change</b>	<b>27%</b>
10. Health and safety	21%	10. Market changes	19%
11. Communications/reputation	20%	11. Fraud	17%
12. Organizational culture	17%	12. Health and safety	17%
13. Market changes	14%	13. Organizational culture	16%
14. Mergers and acquisitions	10%	14. Communications/reputation	14%
15. <b>Climate change</b>	<b>9%</b>	15. Mergers and acquisitions	13%
16. Geopolitical uncertainty	4%	16. Geopolitical uncertainty	12%



Note: The IIA's Risk in Focus Global Survey, North America, n = 442. Percentage who ranked the area as one of their top 5 for audit time and effort.

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

Figure 9:

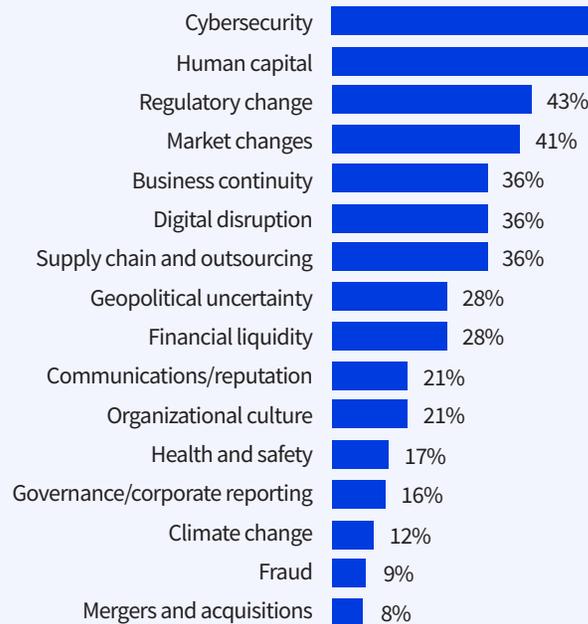
## Current risk levels vs. current audit effort – North America



■ Governance/corporate reporting is low for risk (16%) but high for audit effort (55%).

■ Effort is lower priority compared to risk for geopolitical uncertainty, market changes, and climate change, but these risks may be addressed through financial liquidity, business continuity, or supply chain.

### What are the top 5 risks your organization currently faces?



### What are the top 5 risks on which internal audit spends the most time and effort?



Note: The IIA's Risk in Focus Global Survey, North America, n = 442. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

Figure 10:

## Future risk levels vs. future audit effort – North America



■ Risk levels and effort are expected to be closely aligned in the next 3 years for the growing risk areas of digital disruption (56% to 53%) and climate change (30% to 27%).

What are the top 5 risks your organization will face 3 years from now?

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?



Note: The IIA's Risk in Focus Global Survey, North America, n = 442. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

# CYBERSECURITY

## Team building for cyber resilience

**Because most organizations expect to be hacked, they are focused on building resilience through enterprise-wide collaboration and continuous training.**

The pandemic forced many organizations to rapidly roll out IT systems, often using cloud-based third-party suppliers, to enable staff to work from home during lockdowns. As a result, hacking both intensified and industrialized just at the time when extended networks were most vulnerable. Not only has the risk of state-sponsored cyberattacks increased because of geopolitical uncertainty – including the war in Ukraine and tensions between the U.S. and China – but the burgeoning cyber-attack-as-a-service industry means that amateur hackers can carry out sophisticated scams for a fraction of the time and cost.<sup>2</sup>

Those trends have increased both the potential financial impacts of successful breaches and the risk of existential threat from so-called wiper attacks: experts fear that such knock-out hits currently targeting Ukrainian networks could spread to the U.S.<sup>3</sup> The average cost of a data breach in North America has climbed 12.7% since 2020 to \$4.35 million in 2022, according to IBM. And 83% of respondents said they had experienced multiple breaches, with 45% of those occurring in the cloud.<sup>4</sup>

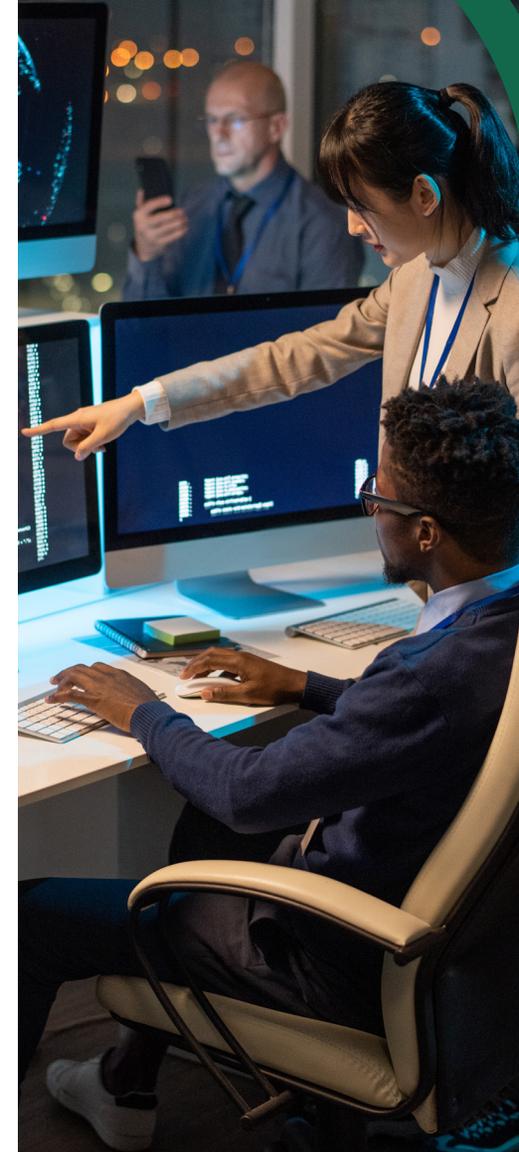
### Survey Results – Cybersecurity

1<sup>ST</sup> – RISK LEVEL

**85%**  
ranked it  
as a top 5  
for risk level

1<sup>ST</sup> – AUDIT EFFORT

**84%**  
ranked it  
as a top 5  
for audit effort



<sup>2</sup> For more about cyber-attack-as-a-service, see <https://fieldeffect.com/blog/cybercrime-as-a-service>

<sup>3</sup> For more about wiper malware, see <https://techcrunch.com/2022/02/28/fbi-cisa-ukraine-wiper-malware/>

<sup>4</sup> For more about cost of data breaches, see <https://www.ibm.com/downloads/cas/3R8N1DZJ>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## CYBERSECURITY

### New SEC rule adds structure

In July 2023, The U.S. Securities and Exchange Commission (SEC) adopted new rules for reporting incidents and disclosing activities related to cybersecurity risk management, strategy, and governance. One of the goals is to make information more consistent and easier to use for decision-makers and investors.<sup>5</sup>

The SEC rules are layered on top of a tangle of existing cyber regulations. There were more than 250 bills or resolutions proposed at state or federal levels in the U.S. in 2021.<sup>6</sup> For those operating across multiple jurisdictions, the time needed to keep up with developments can be significant, said a CAE at a global financial services firm. She described extensive efforts to keep up with requirements, from using cybersecurity consultants to regularly connecting with members of the legal community, the Justice Department, and other CAEs to ensure that the organization is up to speed.

### Cyber defense requires knowledge

Awareness of cyberattacks is high in boardrooms and among executive management, but so are talent shortages for key IT and cyber skills, CAEs at the roundtable said. Posts are hard to fill. It's no wonder that human capital ranked as the second biggest risk, with 65% of survey respondents rating it as a top 5 for risk level (see Figure 1). CAEs from small functions and the public sector say understaffing is particularly acute for them because it is hard to compete with the salaries or career prospects from larger companies and the private sector.

Less well-highlighted is the talent gap in the boardroom. Several CAEs at the roundtable agreed that without specialist IT and cyber knowledge on the audit committee or board, recommendations can fall on deaf ears. “Until you get somebody in that oversight position who genuinely understands what needs to be in a program for cybersecurity

## Resources

[Assessing Cybersecurity Risk: The Three Lines Model](#) (The IIA)

[Auditing Cyber Incident Response and Recovery](#) (The IIA)

[Auditing Cybersecurity Operations: Prevention and Detection](#) (The IIA)

and data protection, who understands the recommendations from the chief information security officer and internal audit, you are not going to get meaningful progress within the company,” said a CAE at a publicly traded North American energy company.



<sup>5</sup> For more about the new SEC rules, see <https://www.sec.gov/news/press-release/2023-139>

<sup>6</sup> For more about cybersecurity legislation in the U.S., see <https://www.ncsl.org/technology-and-communication/cybersecurity-legislation-2021>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## CYBERSECURITY

Some leading organizations elevate the position of chief information security officer (CISO) in the governance structure so that it is easier to pool knowledge, share recommendations, and raise issues. “If the CISO feels there is exposure and the chief information officer refuses to address it, it is critical he or she has the independence to go directly to the CAE or audit committee to be heard,” said Karen Percent, a healthcare industry CAE.

Most CAEs at the roundtable said they were strengthening training and awareness to combat continuous developments in malware and social engineering hacks. They get everyone from the CEO down to entry-level staff to participate in ongoing, faux phishing attacks that incorporate recent hacking methodologies, with extra effort where weaknesses have been identified. Setting the tone at the top and making that visible makes a difference.

Organizations are running through extensive hacking, defense, and recovery scenarios to ensure the executive team and board are ready for strategic decision

“Building good, trusted partnership is the key to everything we do – being flexible, agile, and listening and collaborating with your business partners is essential.”

making if a ransomware attack occurs. This is combined with the use of ethical hackers to test online and operational defense controls.

“You are going to get hacked – it is going to happen,” said an academic from a leading U.S. business school, “so the key focus for the board today is to detect and correct.”

### Collaboration is key to success

Most crucially, collaboration across the entire enterprise is key. Cybersecurity and data security issues are not located

in just one part of a business; they are ubiquitous. That means risks, controls, and mitigations also impact multiple business functions. Ada Leung, vice president and CAE at Fidelity in Canada, said that moving to an integrated assurance model<sup>7</sup> has helped her internal audit department identify and focus on higher risk areas. In addition, migrating to an enterprise-wide technology platform meant that the business was able to employ a single risk taxonomy – one language – across its three lines for IT – another plus.

“Just as a business cannot do things in silos successfully, neither can internal audit,” she said. “Building good, trusted partnerships is the key to everything we do – being flexible, agile, and listening and collaborating with your business partners is essential.”



<sup>7</sup> For more about integrated auditing, see <https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/practice-guide-integrated-approaches-to-internal-auditing/>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## CYBERSECURITY

That also includes listening to staff and watching for potential weak points. Routines that make people’s daily jobs difficult, such as clumsy virtual networks, may be circumvented, creating cyber risk control flash points. Management may try to implement solutions outside of IT oversight, creating a “shadow IT” that is ripe for hacking. One solution is to centralize governance processes for cybersecurity in IT departments and away from management so that IT has full visibility into all technology usage.

CAEs at the roundtable said key internal audit assignments have included:

- Collating IT asset management inventories so that patch programs cover the entire enterprise.
- Assessing cybersecurity maturity of the whole enterprise to create a gap analysis of the controls environment.
- Auditing enterprise-wide risk management to test how complete and effective it is for cybersecurity.

- Collaborating with IT and risk management on creating continuous controls monitoring for both cyber defense and operational controls.

In three years’ time, survey respondents expect that cybersecurity will still be at the top of the list for risk levels and audit effort. With developing technologies, such as artificial intelligence, coming on stream over that time, and the tensions between the U.S. and China over Taiwan, the risk landscape is only likely to become more complex – and potentially more dangerous.

Management may try to implement solutions outside of IT oversight, creating a “shadow IT” that is ripe for hacking.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

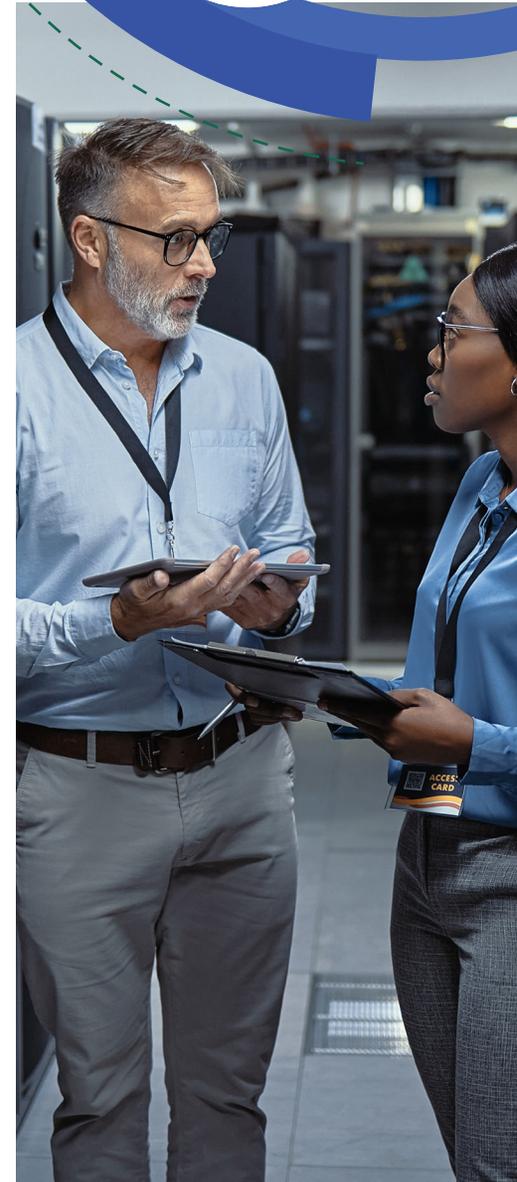
Future expectations:  
Pressure grows from digital disruption  
and climate change



# CYBERSECURITY

## How internal audit can help the organization

1. Assess the level of awareness, knowledge, and skills in key parts of the business, including the board, to ensure that cyber defense responses are relevant and up to date.
2. Evaluate the reporting lines between the CISO, the CIO, and the board to ensure risks and recommendations are communicated clearly and can be escalated to the highest level when necessary.
3. Assess the frequency, timeliness, and effectiveness of faux phishing campaigns and other awareness raising activities and the levels of staff engagement, as well as how well-integrated they are with training and follow-up processes.
4. Use scenario run-throughs to both educate the board on their governance responsibilities and to test that mitigation processes are complete and effective.
5. Evaluate the effectiveness of the controls environment and how well controls are embedded into the first and second lines, paying particular attention to those practices that staff find disruptive or intrusive and are likely to ignore, forget, or circumvent.
6. Evaluate the governance processes around shadow IT and whether it is appropriate for first and second lines to own those technologies and their associated controls.
7. Assess how well the organization's governance structure enables collaboration across the three lines.
8. Assess how well the organization keeps abreast of global developments in cybersecurity and technology regulations reach and how readily data controls can be changed to meet future requirements.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

# HUMAN CAPITAL

## Negotiating the culture clash

**At a time of acute skills and talent shortages, CAEs are helping organizations to diversify work practices, recruitment, and retention strategies.**

Human capital risk cuts across every strategic and operational area of a business. Without the right people, organizations cannot function effectively – either to achieve goals, or to identify, manage, and mitigate key risks. Because of trends such as digitalization and complex emerging risks such as climate change, organizations require a broader and deeper spectrum of expertise across a wider range of areas. But they face critical shortages in essential skills. In cybersecurity alone, one study put the number of unfilled posts in the U.S. at 750,000.<sup>8</sup>

Accelerated by the pandemic, changes to the culture of work have hit hard in North America. The so-called Great Resignation – a process that saw millions of experienced senior workers quit work as lockdowns triggered a re-evaluation of personal priorities – continues. About 4 million people (2.6% of the U.S. workforce) left their posts in October 2022 alone.<sup>9</sup> In addition, many younger people have fallen out of love with the traditional values and corporate work culture. Not only do most insist on flexible employment practices – including hybrid working – but an increasing number value being part of purpose-driven enterprises.<sup>10</sup>



### Survey Results – Human Capital

2<sup>ND</sup> – RISK LEVEL

65%  
ranked it  
as a top 5  
for risk level

8<sup>TH</sup> – AUDIT EFFORT

26%  
ranked it  
as a top 5  
for audit effort



<sup>8</sup> For more about cyber staff shortages, see

<https://www.esentire.com/resources/library/2023-official-cybersecurity-jobs-report>

<sup>9</sup> For more about the Great Resignation, see <https://www.weforum.org/agenda/2023/01/us-workers-jobs-quit/>

<sup>10</sup> For more about hybrid work, see <https://www.mckinsey.com/~media/mckinsey/email/genz/2022/05/17/2022-05-17b.html/> For more about work values, see <https://time.com/6176169/what-young-workers-want-in-jobs/>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## HUMAN CAPITAL

Creating a well-resourced and flexible organizational response is a number-one boardroom priority, CAEs at the roundtable agreed. But that has been made more difficult because of the need to cut costs and fight upward wage demands in an environment that has suffered from inflationary pressures. At the same time, staff are pushing employers to strengthen their diversity, equity, and inclusion (DEI) policies in the workplace. That has seen more firms signing up to voluntarily practice codes proving that they take cultural transformation seriously. In February 2023, more than 100 finance industry organizations across the U.S. and Canada signed up for the industry’s voluntary DEI Code.<sup>11</sup>

### Middle management sets the tone for hybrid work

But not all senior executives are in tune with hybrid work trends. “Some board members are questioning why we are

still hybrid when everybody seems to be returning back to the office,” said a CAE in the U.S. public sector. “But hybrid is a key [option] for us because it helps us attract and retain talent.”

Adopting hybrid working styles is a popular strategy – but it is not without risk. First, without experiencing real-time, in-person events in the workplace, there are fewer opportunities to develop and coach younger staff, said a CAE at a North American professional services firm. As a result, it takes longer for her hires to absorb the values and culture of the business, especially in more distributed organizations. Second, critical soft skills may be less developed in recently graduated joiners – many of whom completed their college years in front of computer screens as higher education went into lockdown. Interestingly, some of those who experienced online-only higher education want to work onsite. Balancing such conflicting preferences is crucial for attracting and retaining staff, CAEs agreed.

Few companies have fully redefined their work processes in the post-pandemic era. Rather than new cultural



## Resources

[Talent Management: Recruiting, Developing, Motivating, and Retaining Great Team Members](#) (The IIA)

[Cultivating a Healthy Culture](#) (Chartered Institute of Internal Auditors)

[2023 Organizational Culture and Ethics Report](#) (AuditBoard)

expectations being set by the board, culture is more likely to be defined by middle management out of necessity, said Brian Tremblay, CAE at 1stDibs. “Corporate culture is defined by the ‘tone in the middle,’ where managers make decisions for the benefit of their people, which may or may not align to the organization’s values,” he said. CAEs can help by providing boards with awareness about differences in work practices across business units so that boards are more in tune with culture realities.

<sup>11</sup> For more about the finance industry DEI Code, see <https://www.cfainstitute.org/en/about/press-releases/2023/dei-code-100-signatories-milestone>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## HUMAN CAPITAL

### Diversity is more than skin deep

A variety of research has shown a positive correlation between increased diversity and economic growth in both the general U.S. economy and in individual businesses.<sup>12</sup> Many organizations have embraced those findings, as has the U.S. federal government, which is implementing new DEI requirements for federal bodies.<sup>13</sup>

Several CAEs at the roundtable said their boards expect their organizations to make extensive use of diversity and inclusion metrics. A CAE at a retail bank said her organization goes beyond tracking physical attributes and also considers diversity in thought, approach, and mindset. Some organizations use the DiSC personality test to better understand the working styles of their employees and maximize employee effectiveness.<sup>14</sup>

Yet while tracking diversity has benefits, caution must be taken to avoid triggering legal action if the statistics

Several CAEs at the roundtable said their boards expect their organizations to make extensive use of diversity and inclusion metrics.

demonstrate that some groups have been discriminated against.

### Look for non-traditional signs of trouble

Auditing policies, procedures, and the results of employee surveys are obvious internal audit assignments, but they can miss the less obvious signs of trouble. Internal audit can use thoughtful observations to pick up on less-tangible signals – low morale, negative social media, messy breakrooms – and explore whether these are signs of deeper cultural problems.

### Collaborate to break down siloed recruitment

A CAE in the education industry echoed a growing sentiment when he said that he had stopped looking at internal audit as a silo within the organization. Instead, he overhauled his department's human resources framework to drop the pretense that internal audit had to be a career for life and ensured that he collaborated with other departments to help improve overall staff retention since all areas of the business are suffering the same challenges.

<sup>12</sup> For more about the positive correlation between diversity and performance, see <https://hbr.org/2018/07/the-other-diversity-dividend>

<sup>13</sup> For more about the statement on DEI, see <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/25/executive-order-on-diversity-equity-inclusion-and-accessibility-in-the-federal-workforce/>

<sup>14</sup> For more about DiSC, see <https://www.discprofile.com/products/everything-disc-workplace-profile>



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## HUMAN CAPITAL

Boosting rotations from within the business, increasing the use of guest auditors for specific assignments, and openly discussing new applicants' longer-term career choices helped ease pressure in the internal audit function. "I'm playing the longer game by helping people stay at the business and benefit from an environment of learning, which seems to be working," he said.

Similarly, a CAE at a global analytics company said that his staff often make lateral moves within the organization as a result of having close contact with many business units. Despite the extra effort needed to backfill the internal audit positions, he believes the moves ultimately improve the overall risk maturity of the business.

### Capitalize on strengths for internal audit recruiting

While CAEs said they were working to help organizations create the right culture to attract, train, and retain staff within

"I'm playing the longer game by helping people stay at the business and benefit from an environment of learning..."

their organizations, many are hampered by staff and skills shortages in their own audit functions – particularly in smaller organizations and the public sector, where budget pressures can be intense.

Although public sector organizations often struggle to offer competitive pay, they can emphasize their public service ethos to increase recruitment and retention, said Pamela Stroebe Powers, The IIA's director of professional guidance for the public sector. "Organizations must set performance expectations up front and make sure people understand how their job relates to the purpose of the organization because every single job in the organization should relate to that mission."



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## HUMAN CAPITAL

### How internal audit can help the organization

1. Evaluate how well management has identified the potential emerging risks of hybrid working and has developed effective strategies and policies to mitigate those risks.
2. Assess the varieties of corporate cultural practices throughout the business and communicate those to the board to feed into decision making and policy setting.
3. Assess the use of formal diversity metrics and their effectiveness in monitoring diversity and inclusion policies, including whether they consider diversity of thought and mind.
4. Develop strategies to use personal interactions with audit clients to identify intangible signs that cultural problems may be brewing and capture those observations for follow up and remediation.
5. Evaluate whether the organization's human resources framework aims to attract and retain talent within the enterprise – rather than within individual silos – and that career progress paths are well-structured and clearly communicated.
6. Assess whether the organization's broader purpose is well-defined and communicated throughout the enterprise, including in human resources strategies for attracting and retaining staff.



## Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

# MARKET CHANGES

## Adding value with strategic involvement

**Markets are changing unpredictably, causing organizations to invest in digital strategies that are more responsive to fast-moving trends. CAEs are bringing together expertise across their businesses and acting as advisors on new initiatives to help those transformations.**

The economy in North America has driven market changes, competition, and changing consumer behavior over the past year. At the beginning of 2022, the U.S. Federal Reserve turned its attention away from the pandemic to containing inflation, signaling the end of an era of historically cheap money. Business bankruptcies rose as pandemic help faded and customers cut back spending in the face of higher prices.<sup>15</sup> Inflation and a rising dollar made products manufactured in North America more expensive, squeezing domestic margins and

pushing imports – especially from China – to pre-pandemic levels.<sup>16</sup> In financial services, some banks collapsed partly because they failed to manage interest rate risk.<sup>17</sup>

At the same time, organizations are adapting to longer-term trends in digital consumerism. Young people have transformed the way consumers interact with organizations – from shopping and service use to activism and public criticism. In a less loyal, more socially connected marketplace, reputations can crash and trigger bank runs in a matter of hours.

### Survey Results – Market Changes

4<sup>TH</sup> – RISK LEVEL

**41%**  
ranked it  
as a top 5  
for risk level

13<sup>TH</sup> – AUDIT EFFORT

**14%**  
ranked it  
as a top 5  
for audit effort



<sup>15</sup> For more about U.S. bankruptcy metrics, see <https://tradingeconomics.com/united-states/bankruptcies>

<sup>16</sup> For more about global trade, see <https://www.globaltradedmag.com/increase-in-u-s-container-import-volumes-makes-2023-look-more-like-2019/>

<sup>17</sup> For more about bank failures, see <https://www.nytimes.com/article/svb-silicon-valley-bank-explainer.html>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## MARKET CHANGES

### Early involvement prevents future problems

Rapidly investing in the technology to deliver products and services is often essential to keep up with the market, CAEs at the roundtable said. But doing so increases exposure to other threats, including cybersecurity for new and untried systems and supply chain risk where services move to the cloud or change their operating structure.

That is why it is critical for CAEs to be involved at the implementation stage as advisors, said Ada Leung, vice president and CAE at Fidelity in Canada. “It is no longer enough to come back three years after a project has been launched and make sure the controls were good. Nowadays, we are collaborating and partnering with the partners to provide assurance of design controls prior to implementation. It is a much safer, cheaper, and more effective approach.”

“Market changes are dynamic risk events in themselves, so CAEs must constantly be alert to re-evaluate what they are auditing and how.”

But devising an audit plan for a digitally transforming organization is challenging. “CAEs must be clued into organizational strategies, which means not conducting static risk assessments nor having an event-based audit plan that is inflexible,” said Harold Silverman, The IIA’s senior director of CAE and corporate governance engagement. “Emerging technologies, market changes are dynamic risk events in themselves so CAEs must constantly be alert to re-evaluate what they are auditing and how.” Rather than simply focusing on separate engagements, Silverman said CAEs must update their audit assignments regularly to include those new elements in the audit department’s planned work schedule.

That makes sense, first, because risks related to market changes are often embedded in other types of threat, for example, liquidity and financial risk. Second, incorporating market risks into the planned work schedule may enable a CAE to cover that risk without needing to broach it with a reluctant audit committee – even though upward education in risk is an important function of the CAE. Finally, it prevents the internal audit department from neglecting upcoming threats due to an out-of-date audit plan or slow methodologies that do not suit the risk category, he said.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## MARKET CHANGES

### Calculate the costs of market risks

Organizations need to do more than just identify market risks; they should calculate accurate and specific information about financial impacts, said a CAE at a non-profit healthcare organization. “My goal is to get to ‘What is our unmitigated risk in dollar terms?’ in a way that our executive leadership team can decide which strategic initiatives we are going to pursue or not pursue.”

Ayaka Mitsunari, internal audit director/risk architect for delivery at Uber, said her team reviews governance processes, strategy, and operating structures to assess whether the business is able to respond effectively to market challenges. For example, internal audit asks, “How is management measuring the stickiness of the product? Do they have the right processes to be able to adapt quickly and innovatively?” she said.

### Bring in experts when needed

Given the interconnected nature of the risk and its mitigation strategies, collaborating across the business by tapping into sources of knowledge is key to success. “With accelerated change in markets and customer trends, the future for internal audit and risk management professionals is to be able to partner with senior management on addressing a risk six months from now that you probably have not identified yet. You are going to have to pivot and be flexible,” said a leading academic at the roundtable.

“We do not have [all] the answers in these emerging areas, so we need to be humble, learn, and be attuned to those risk areas where we need to bring in

experts if there is a deficiency in the business,” Nancy Russell, CAE at Canada Life. “That could rub against executive egos, but it is important to encourage them to be transparent with the board where solutions do not exist and be open to bringing in help where needed.”

To build business knowledge, CAEs at the roundtable said they strive to hire from a more diverse cohort of staff, especially those with business acumen and experience – although current skills and talent shortages makes that task difficult. To expand internal audit’s range and depth of skills, they also said they focused on boosting certification and training, as well as rotating people through the department and making use of guest auditors on technical issues.



# Contents

Executive summary – North America

---

Methodology

---

Survey results: Global

---

Survey results: North America

---

Cybersecurity:  
Team building for cyber resilience

---

Human capital:  
Negotiating the culture clash

---

Market changes:  
Adding value with strategic involvement

---

Business continuity:  
Building resilience in complexity

---

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

---

Future expectations:  
Pressure grows from digital disruption  
and climate change

## MARKET CHANGES

### How internal audit can help the organization

1. Evaluate the organization's risk management to see if there are adequate horizon-scanning processes to track emerging market trends and use them for strategic decision making.
2. Provide input on market-driven technology projects at the implementation stage to ensure risks are properly assessed and mitigated.
3. Assess how effectively risks from market changes, competition, and consumer behavior are quantified in monetary terms and used in decision-making processes.
4. Assess how well the overall governance processes in the business are responsive to market changes and able to pivot to take advantage of new opportunities.
5. Evaluate the organization's human resources strategies to ensure that key skills and expertise relating to future risks and opportunities are identified – including in the internal audit department – and recruited for in a timely way.



## Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

# BUSINESS CONTINUITY

## Building resilience in complexity

**If boards tended to under-prioritize business continuity plans before the pandemic, that is no longer the case. High-profile cyber breaches, extreme weather events, and rising geopolitical tensions – particularly between the U.S. and China – continue to keep the topic on the agenda.**

In fact, business continuity, operational resilience, crisis management, and disaster recovery are often not seen as risks in themselves, but as a response to a wide range of potential interruption to the business. “For the systemic risks we face and threats such as supply chain disruption and vendor resiliency, we feel like the answer to all these different things is having a business continuity plan,” commented a CAE from a U.S. manufacturer.

### Event-based planning is too narrow

The experience of the pandemic and the rapid macroeconomic changes that have driven up inflation and interest rates has not only made it a boardroom imperative to better prepare organizations for the future, but also altered the way businesses think about operational resilience.



### Survey Results – Business Continuity

5<sup>TH</sup> – RISK LEVEL

**36%**  
ranked it  
as a top 5  
for risk level

3<sup>RD</sup> – AUDIT EFFORT

**53%**  
ranked it  
as a top 5  
for audit effort



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## BUSINESS CONTINUITY

In particular, CAEs at the roundtable agreed that the pandemic mostly overwhelmed those business continuity plans that did exist because of the scale and complexity of the event. Public sector bodies, for example, had to distribute government aid immediately without fraud controls in place. In addition, suppliers, partners, and customers were equally affected so that business continuity plans often failed to account for disruption to those organizations they would normally turn to for support.

“My organization had done a lot of disaster preparedness and planning for local disasters, but this hit everyone all at once, so organizations were not prepared for cross-functional, cross-jurisdictional emergencies of such magnitude,” said Pamela Stroebel Powers, director of professional guidance for the public sector at The IIA. Organizations have learned that rapid, unpredictable knock-on risks are a core feature of systemic risks. That means that disasters that are systemic – rather than triggered by a single event, like a storm – fundamentally alter the way that risk can be managed and mitigated during a crisis.

Organizations must plan for both event-based and non-traditional, broad-scope crises. Shannon Urban, vice president and CAE at Hasbro, said her business extended its enterprise risk program to include both types of risk and internal audit ensures they are included, monitored, and that disaster recovery plans are in place. In addition, disaster recovery plans go through regular desktop exercises, where internal audit provides a critical voice so that any weaknesses are proactively identified and tackled.

### Detailed risk assessments need deeper collaboration

Given that macroeconomic and geopolitical uncertainty, changes in market behavior, climate change events, and cybersecurity risk share similar characteristics of speed, scale, and complexity, organizations are redrawing the parameters of their disaster response plans and focusing more on

organizational resilience. Some CAEs at the roundtable said they felt they were currently in permanent crisis mode, but with limited resources. In some sectors, regulators are pushing for organizations to take a longer-term view of their viability.

Organizations must plan for both event-based and non-traditional, broad-scope crises.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## BUSINESS CONTINUITY

“Although the rate of change feels fast now, this is probably the slowest time we will ever operate in as developments such as AI will accelerate faster,” said Nancy Russell, CAE at Canada Life. “We need to find out what we and the regulators are comfortable with and what operational resilience means in practice – and because of the dynamics of change in the organization, we have to become comfortable with being uncomfortable as well.”

As part of those efforts, organizations must recalibrate risk assessments to creatively connect apparently unrelated or unexpected threats that could combine to interrupt the business. For example, a CAE at a U.S. technology company said 80% of his business’s chip-manufacturing capacity was based in Taiwan, which is under potential threat from China. He had been using tabletop scenario-planning to build up an accurate picture of how the company could pivot to meet customer demand in light of possible war, sanctions, or supply chain disruption. “Having continuity plans and resiliency practices in place to either react to or prepare in advance has really helped

focus the board about resilience at a strategic level,” he said.

Building rich detail into such scenarios is critical because the mitigations that arise as a consequence of dealing with threats can themselves create second and third order risks that need to be mitigated – but that entails collaborating more deeply with management on what can go wrong. “We have made our risk assessment meetings bigger when it comes to crises because it helps management really prepare for longer-term issues,” a CAE at a higher education establishment said. Without working together to build such granular, data-driven plans, organizations will flounder when disaster strikes.

“It is more important than ever to meet managers face to face and take the pulse of what keeps them up at night, as well as share what internal audit is monitoring,” Hasbro’s Urban said. “Nine times out of ten, you do not need a formal audit to drive change – you just need to convince the right people that the problem is really something they should be thinking about.”



## Resources

[Business Continuity Management \(The IIA\)](#)

[Navigating Geopolitical Risk \(Chartered Institute of Internal Auditors\)](#)

[Auditing Third-Party Risk Management \(The IIA\)](#)

CAEs at the roundtable said they also supported the robustness of risk assessments, governance structures, and relevance of business continuity plans, as well as testing whether the resources are in place to carry out the plan should disaster strike. Many said they implemented a form of combined assurance for their business continuity planning, and some said they co-sourced with external experts and suppliers to make sure they had as few gaps as possible in the range of events covered and in their plans.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## BUSINESS CONTINUITY

### Planning ahead to fill talent is key

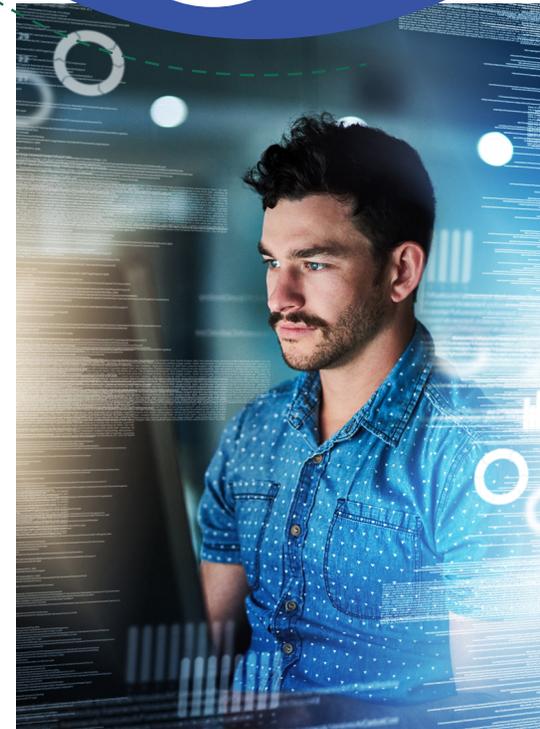
The complexity of such large-scale threats requires operational continuity planning based on high levels of expertise that businesses often do not have in the current human resources crisis – human capital, diversity, and talent management and retention ranked as the second biggest threat in the survey. Key skills and talent are in short supply. Lean business models and automation have stripped out some of the resources needed for such detailed work, said CAEs at the roundtable.

In addition, succession planning for key management posts is an emerging risk. It is common for hard-to-fill, senior vacancies to be open for over a year, especially in areas such as IT and in many other specialties in smaller businesses and public sector organizations. “We are trying to do more and more with less, so we are unable to offer marketable salaries,” a CAE at one university said. “There is no succession plan in place for key roles and it is really impacting

business continuity.” If those positions are not filled when an emergency arises, the business continuity plans will not work. Someone must be in place who will take responsibility and has practiced the response plan.

Preparing for regulations on emerging risks that could disrupt the business or its supply chains, such as future U.S.- Chinese sanctions, require organizations to hire expertise in advance. The CAE at the Taiwan connected manufacturing business said that his company was shifting more to software development and needed not only to hire for a strategic change of direction, but also to ensure the company had the regulatory expertise to feed into its business continuity planning exercises.

Most CAEs at the roundtable said they were working to embed business continuity topics in all future internal audits – although the two biggest emerging risk areas – digital disruption and climate change – are both potentially business continuity issues that may demand more attention than expected.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## BUSINESS CONTINUITY

### How internal audit can help the organization

1. Evaluate how comprehensively the organization's enterprise risk management framework includes both event-based and large-scale disruptive risks.
2. Compare regulatory requirements with the organization's risk appetite to establish a suitable strategy for business continuity planning.
3. Help identify second-order or third-order risks that may arise in complex risk scenarios or because of the negative impact of first-order risk mitigation steps in the business continuity plan.
4. Review business continuity processes to ensure a wide range of voices and expertise contributes to brainstorming and plan creation to foster a longer-term outlook.
5. Support management by providing a critical independent voice at tabletop exercises to evaluate their completeness and to highlight where risk mitigation plans need additional resources or testing.
6. Provide assurance that the resources and personnel identified in disaster recovery and crisis management plans are in place and that the processes and controls that support those plans exist and work during real-time exercises.
7. Evaluate the organization's human capital needs for effective business continuity planning, including the existence of key personnel, expertise in emerging risk areas, and in the internal audit department.



## Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



PAGE 40 OF 49

# INTERCONNECTED RISKS

## Geopolitical uncertainty, supply chain, and regulatory change

**Efforts to deal with the widespread impacts of emerging global risks are being hampered by increased regulatory requirements. CAEs are seeking better alignment with risk management in complex areas such as supply chain disruption.**

### Engage in strategic planning discussions for geopolitical uncertainty

CAEs at the roundtables said that many U.S. Fortune 100 companies had the risk of war on their radar. Influenced by the unexpected invasion of Ukraine by Russia in 2022 and rising tensions with China, organizations have strengthened cybersecurity defenses and revisited risk assessments, mitigations, and scenario testing across a wide range of inter-related threats, they said.

Yet, like many interconnected threats in this report, it would be a mistake to consider macroeconomic and geopolitical risk simply as an individual risk category. If Brazil, Russia, India, China, and South Africa, for example, launched a much-discussed

alternative global currency, it could, like other geopolitical decisions, be a key driver for a basket of associated risks that could hit North American businesses unpredictably, fast, and simultaneously across their whole enterprises.<sup>18</sup>

So, while this category ranked low in terms of audit time and effort, those efforts are most likely distributed in activities that may not be on the audit plan, such as stress testing, scenario analysis, and strategic advice.

A CAE from a leading North American global consultancy said: “There is a difference between what is auditable on your audit plan, versus what you’re involved with in the organization, especially when you are in the strategic planning meetings.” He said that CAEs must act as strategic enablers for the board so that they can make informed, rapid decisions in such fast-moving but long-term risk scenarios.



“There is a difference between what is auditable on your audit plan, versus what you’re involved with in the organization, especially when you are in the strategic planning meetings.”

<sup>18</sup> For more about BRICS currency, see <https://foreignpolicy.com/2023/04/24/brics-currency-end-dollar-dominance-united-states-russia-china/>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## INTERCONNECTED RISKS

### Diversify the supply chain before crisis strikes

While the pandemic exposed weaknesses to global supply chain networks as ports closed and trade flow stuttered, North America is still dependent on China for much of its manufacturing. In 2023, China produced 28.4% of global manufacturing output compared with 16.6% for the U.S. – in dollars, \$4 trillion and \$1.8 trillion, respectively.<sup>19</sup> Recent events have highlighted that too many organizations suffer concentration risk among key suppliers. That may be one reason political rhetoric has switched from decoupling with China to the diversification and resilience of supply chains.<sup>20</sup> The challenge is not simply one of finding a manufacturer in a different location but, more crucially, it is to pivot the whole operational infrastructure to avoid potential logistical and quality issues.<sup>21</sup>

For example, when global toy and games company Hasbro began diversifying

“You can’t just pick up expertise for manufacturing high-quality products from a country that has been doing it for 50 years and transplant it into a country that has been doing it for 10.”

away from China several years ago, it needed to invest heavily across its entire operational infrastructure and with third-party partners. “You can’t just pick up expertise for manufacturing high-quality products from a country that has been doing it for 50 years and transplant it into a country that has been doing it for 10,” said Shannon Urban, vice president and CAE at Hasbro. Partnering to train staff at suppliers and duplicating tooling in multiple locations has both smoothed the process and introduced extra resilience into the business.

The initiative at Hasbro sat underneath a broader, management-run transformation program across the



whole supply chain infrastructure to strengthen resiliency throughout the business – a major strategic project. Given that automation was a key component of the initiative, internal audit engaged with the project to provide advice on the design of effective controls for those systems and redesigned processes and controls from the outset. This kind of work requires a different skillset from traditional internal audit, so Hasbro has invested in competency assessment, training, and on-the-job coaching for the audit team.

<sup>19</sup> For more about U.S. Statistical Division analysis of manufacturing, see <https://worldpopulationreview.com/country-rankings/manufacturing-by-country>

<sup>20</sup> For more about the statement on diversifying, see <https://www.reuters.com/world/cias-burns-us-needs-de-risk-diversify-away-china-2023-07-01/>

<sup>21</sup> For more about the challenges of moving manufacturing, see <https://asiatimes.com/2023/06/why-so-much-manufacturing-still-gets-done-in-china/>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



PAGE 42 OF 49

## INTERCONNECTED RISKS

### Seek alignment and help on conflicting risks

CAEs at the roundtable agreed that regulation was complicating supply chain restructuring. The rise in expected risk for regulatory change is likely fueled by the proliferation of European-style data protection laws across North America. Unlike in Europe where the General Data Protection Regulation of 2018 is implemented with few changes by countries within the region, North American legislators have taken those concepts and enacted widely different rules from state to state, creating a patchwork of often-conflicting compliance requirements.<sup>22</sup>

“We have reached a situation where providing absolute assurance on data privacy laws is so cost prohibitive that it is basically impossible,” said Brian Tremblay, CAE at 1stDibs. He compared the current situation with data privacy to the early days of SOX compliance, where the area was so over-controlled that it soaked up too much internal audit effort.

CAEs at the roundtable agreed that internal audit’s time is getting too divided to deal effectively with simultaneous emerging risks and burgeoning compliance. “Just as we are responding to these changes in consumer behavior and investing in technology, the pace of regulatory change at a federal and state level has gone berserk,” said a CAE in the healthcare industry. That pressure had made her organization more reactive, she believes, pointing to one reason that internal audit time is often being redirected to regulatory compliance.

Aligning internal audit and risk management is critical, Tremblay said. Like many CAEs of publicly listed companies, he has responsibility for risk management. As part of the role, he helps define risk appetite and privacy policies as well as document how those decisions can provide better clarity on the organization’s stance. Collaborating with IT to use enterprise-wide technology solutions to embed privacy controls must be a key strategy if internal auditors are not to be swamped with compliance-related work, he added.



<sup>22</sup> For more about the data privacy laws to be implemented in 2023, see <https://secureprivacy.ai/blog/2023-us-consumer-privacy-laws>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## INTERCONNECTED RISKS

### How internal audit can help the organization

1. Support the board in strategic planning to help enable risk-informed decision making on emerging and fast-moving geopolitical and economic risks.
2. Assess the organization's processes to identify, assess, and build mitigation strategies for complex geopolitical risks and encourage them to pay attention to the interconnections between risk categories.
3. Evaluate the organization's supply chain strategy, including whether it has adequately assessed the risks associated with in-country critical infrastructure when relocating regions.
4. Assess the organization's relationship with critical suppliers and evaluate the need for a more collaborative approach around training and capacity building.
5. Evaluate the communication between risk management and internal audit to better align on emerging risks.
6. Assess the maturity of the organization's automated controls systems to help reduce the burden of regulatory compliance.



# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



# FUTURE EXPECTATIONS

## Pressure grows from digital disruption and climate change

**Two areas stood out dramatically for expected increases in risk and audit effort – digital disruption and climate change. CAEs are helping their organizations better understand and manage such and helping to keep a strategic focus.**

Rapid developments in artificial intelligence in 2023 were highlighted by the huge media coverage of Open AI’s algorithm ChatGPT, a program that creates written documents on request.<sup>23</sup> Roundtable participants said they had been carefully experimenting with the program. “We have been using ChatGPT just to pose questions, get some context, and write papers,” a CAE at a retail chain said. “We have even used it for some of the board narratives and write up, but with a lot of caution.” None relied on it completely for developing documents, but a CAE at a non-profit healthcare business said it had expedited his research and report writing.

The attraction is obvious – such technologies can improve productivity, competitiveness, and, at a time of higher production costs and a cost-of-living crisis, improve margins. But CAEs at the roundtable agreed users do not always understand potential risks, such as breaching data compliance laws or introducing bias into decision-making processes. Because such technologies are easy to download and use, keeping abreast of those risks is difficult.

### Survey Results – Future Expectations

DIGITAL DISRUPTION

Risk rank  
increased from  
**9<sup>th</sup> TO 2<sup>nd</sup>**

CLIMATE CHANGE

Risk rank  
increased from  
**15<sup>th</sup> TO 9<sup>th</sup>**



<sup>23</sup> For more about ChatGPT, see <https://www.sciencefocus.com/future-technology/gpt-3/>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change



## FUTURE EXPECTATIONS

### Audit emerging IT risk at the speed of technology

“The key challenge for internal auditors is to ensure they audit at the speed of technology because disruptive technologies typically do not have the policies, procedures, methodologies, risk assessments, and mitigations that are in place for more established IT,” said Harold Silverman, The IIA’s senior director of CAE and corporate governance engagement. This requires not only being present with the right knowledge when such projects start within the business, but also hiring the right skills into the audit department.

“Instead of just talking about risk from a negative viewpoint, CAEs should be willing to have a conversation about what the potential advantages are to a greater ESG focus.”

Getting a grip on data governance is key. Data governance can be hard to understand in fast-moving businesses, the focus group agreed. That has led some organizations to break down their definitions of governance into more manageable chunks – IP data governance, privacy-related data governance, and so on. Looking across different audits at these smaller topics can help, as can embedding data privacy controls into automated processes.

### Climate change risk reporting needs strategic view

Having accurate data and reporting lines will be critical when businesses begin to tackle climate-related risks. Enhanced disclosure is in the pipeline from the SEC, with so-called large, accelerated filers (businesses with \$700 million public flotation) having to file on greenhouse gas emissions and other metrics from fiscal year ended 2023.<sup>24</sup> Smaller companies begin filing in 2024. But North American businesses are less active in

## Resources

[Auditing Privacy Risks](#) (The IIA)

[Harnessing Internal Audit Against Climate Change Risk](#) (Chartered Institute of Internal Auditors)

this area than other regions in the world. With so many pressing high-level risks on corporate agendas, CAEs need to tread carefully in order to educate the board and start conversations that will help them prepare.

“CAEs should be open minded in terms of assessing risks related to ESG topics and talking to executives and their boards about those risks, even from a strategic point of view,” says Richard Chambers, senior audit advisor at AuditBoard. “Instead of just talking about risk from a negative viewpoint, CAEs should be willing to have a conversation about what the potential advantages are to a greater ESG focus.”

<sup>24</sup> For more about SEC climate-related rules, see <https://www.sec.gov/files/33-11042-fact-sheet.pdf>

# Contents

Executive summary – North America

Methodology

Survey results: Global

Survey results: North America

Cybersecurity:  
Team building for cyber resilience

Human capital:  
Negotiating the culture clash

Market changes:  
Adding value with strategic involvement

Business continuity:  
Building resilience in complexity

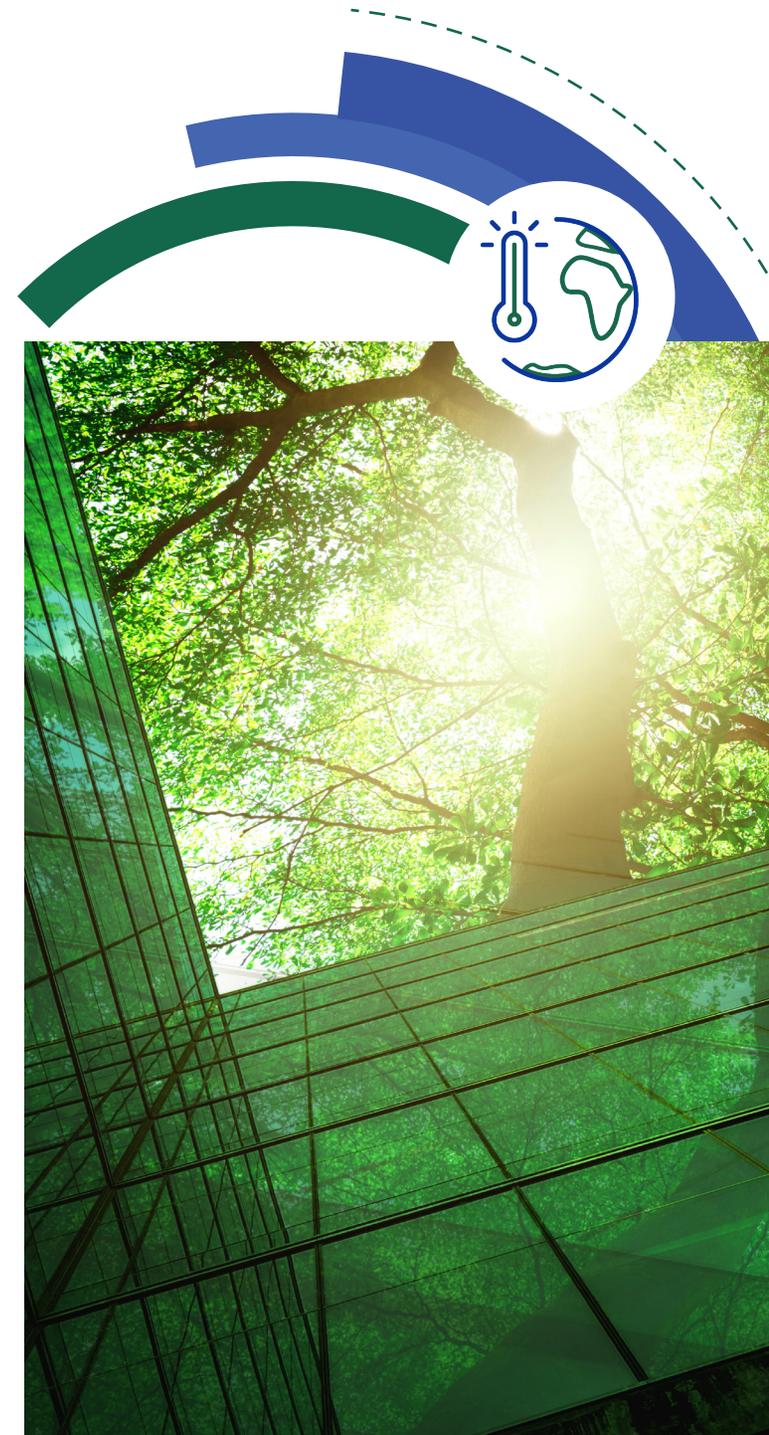
Interconnected risks:  
Geopolitical uncertainty, supply chain,  
and regulatory change

Future expectations:  
Pressure grows from digital disruption  
and climate change

## FUTURE EXPECTATIONS

### How internal audit can help the organization

1. Engage with management on emerging technologies to provide risk and controls advice on the implementation of new systems.
2. Evaluate how management structures and thinks about data, including whether the data taxonomy is granular enough to identify and mitigate appropriate risks.
3. Provide assurance that the business identifies core IT systems and processes that can be used to embed privacy and data controls to reduce the compliance burden across the three lines.
4. Evaluate the completeness and accuracy of data processes in the organization that relate to ESG issues, with particular attention to forthcoming regulatory compliance requirements on climate-related disclosures.
5. Proactively broach ESG-related issues – and other emerging risks – with the board, emphasizing the potential upsides of taking a proactive, early-adopter strategic position.



# ACKNOWLEDGMENTS

## North America Report Development Team

### Project directors

**Laura LeBlanc** –

Senior Director, Internal Audit Foundation

**Deborah Poulalion** –

Senior Manager, Research and Insights, The IIA

**Emely Katz** –

Director, Affiliate Engagement, The IIA

### Survey analysis and content development

**Deborah Poulalion** –

Senior Manager, Research and Insights, The IIA

### Research writer

**Arthur Piper** – Smith de Wint, United Kingdom

### Graphic designer

**Cathy Watanabe**

### Roundtable moderator – North America

**Harold Silverman** –

Senior Director, CAE and Corporate Governance Engagement, The IIA

### French translation

**IIA–Canada**

### North America Report Sponsor

**AuditBoard**

### Cover photo

Nova Scotia, Canada, courtesy of Getty Images

## Internal Audit Foundation 2023–24 Board of Trustees

### President

**Warren W. Stippich Jr.**, CIA, CRMA

### Senior Vice President – Strategy

**Glenn Ho**, CIA, CRMA

### Vice President – Finance and Development

**Sarah Fedele**, CIA, CRMA

### Vice President – Content

**Yulia Gurman**, CIA

### Trustees

**Hossam El Shaffei**, CCSA, CRMA

**Reyes Fuentes Ortea**, CIA, CCSA, CRMA

**Nora Kelani**, CIA, CRMA

**Shirley Livhuwani Machaba**, CCSA, CRMA

**Raoul Ménès**, CIA, CCSA, CRMA

**Hiroshi Naka**, CIA

**Anthony J. Pugliese**, CIA

**Bhaskar Subramanian**

### Staff liaison

**Laura LeBlanc** –

Senior Director, Internal Audit Foundation

## Internal Audit Foundation 2023–24 Committee of Research and Education Advisors

### Chair

**Yulia Gurman**, CIA

### Vice-Chair

**Jane Traub**, CIA, CCSA, CRMA

### Members

**Tonya Arnold-Tornquist**, CIA, CRMA

**Christopher Calvin**, CIA

**Jiin-Feng Chen**, CIA

**Andre Domingos**

**Christina Duquette**, CRMA

**Marc Eulerich**, CIA

**Dagmar Flores**, CIA, CCSA, CRMA

**Anargul Kairulla**, CIA

**Ayaka Mitsunari**

**Ahmed Mohammed**, CIA

**Grace Mubako**, CIA

**Ruth Doreen Mutebe**, CIA

**Erika C. Ray**, CIA

**Brian Tremblay**, CIA

**Koji Watanabe**

### Staff liaison

**Deborah Poulalion** –

Senior Manager, Research and Insights, The IIA



# SPONSORS

## FOUNDATION STRATEGIC PARTNERS



## Foundation Partners



## Gold Partners

**Larry Harrington**  
CIA, QIAL, CRMA

**Stacey Schabel**  
CIA



## RISK IN FOCUS PARTNERS

- |                          |                 |                    |
|--------------------------|-----------------|--------------------|
| IIA – Argentina          | IIA – Ghana     | IIA – Peru         |
| IIA – Australia          | IIA – Guatemala | IIA – Philippines  |
| IIA – Bolivia            | IIA – Hong Kong | IIA – Rwanda       |
| IIA – Brazil             | IIA – Indonesia | IIA – Singapore    |
| IIA – Chile              | IIA – Japan     | IIA – South Africa |
| IIA – Colombia           | IIA – Kenya     | IIA – Tanzania     |
| IIA – Costa Rica         | IIA – Malaysia  | IIA – Uganda       |
| IIA – Dominican Republic | IIA – Mexico    | IIA – Uruguay      |
| IIA – Ecuador            | IIA – Nicaragua | IIA – Venezuela    |
| IIA – El Salvador        | IIA – Panama    |                    |
|                          | IIA – Paraguay  |                    |



# Future Focused.

**Support our Academic Fund programs,  
grants & scholarships.**

An investment in the Academic Fund is an investment in the future of the profession of internal auditing. Contributions provide professors and students an opportunity to access the resources needed to promote and study internal auditing globally. Generous donors help ensure the future of the profession.

**Donate Now.** [theiia.org/IAFdonate](https://theiia.org/IAFdonate)



# ABOUT THE IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 235,000 global members and has awarded more than 190,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit [theiia.org](https://theiia.org).

## About the Internal Audit Foundation

The Internal Audit Foundation provides insight to internal audit practitioners and their stakeholders, promoting and advancing the value of the internal audit profession globally. Through the Academic Fund, the Foundation supports the future of the profession through grants to support internal audit education at institutions of higher education. For more information, visit [theiia.org/Foundation](https://theiia.org/Foundation).

## Disclaimer and Copyright

The IIA publishes this document for informational and educational purposes. This 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 seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright © 2023 by the Internal Audit Foundation. All rights reserved. For permission to republish, please contact [Copyright@theiia.org](mailto:Copyright@theiia.org).



Global Headquarters | The Institute of Internal Auditors  
1035 Greenwood Blvd., Suite 401 | Lake Mary, FL 32746, USA  
Phone: +1-407-937-1111 | Fax: +1-407-937-1101  
Web: [theiia.org](https://theiia.org)



March 5, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Richard P. Bendall   
Chief Audit Executive

Nathan K. Amick   
Senior Internal Auditor

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Fiscal Year Ending 2024 Audit Plan Status Report**

### **BACKGROUND**

According to the Institute of Internal Auditor's (IIA's) *International Standards for the Professional Practice of Internal Auditing (Standards)*, Standard 2010, "the Chief Audit Executive (CAE) must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals. This requirement is also stated in the Audit Committee Charter (Charter). In alignment with the Standards and the Charter, the Audit Committee approved the FYE 2024 Audit Plan (Audit Plan) at its June 2023 meeting.

As of the December 2023 meeting, the Audit Plan consisted of 29 Projects. As of March 5, 2024, Internal Audit staff has completed 9 (31%) of the 29 projects, and 10 (34%) are current and continuous, resulting in a total 19 (65%) completed or current and up-to-date. Of the 10 remaining projects, 4 (14%) are currently in progress, and 6 (21%) have yet to be started.

Staff has prepared the following attachments for your attention:

- A. FYE 2024 Audit Plan as of March 5, 2024
- B. FYE 2024 Audit Plan presentation detailing the worked performed as of March 5, 2024

# ATTACHMENT A

FYE 2024 INTERNAL AUDIT PLAN				
ENTERPRISE RISK MANAGEMENT (ERM) PLAN				10 Percent
ERM TASKS				BASIS FOR INCLUSION
1	ERM Program Plan			Strategic Plan
AUDIT PLAN				90 Percent
	DIVISION	AUDIT / PROJECT NAME	PROJECT TYPE	STATUS
EXECUTIVE/LEGAL/ORGANIZATIONAL				
1	Exec Office	Records & Info Mgmt (FKA: Document Retention)	Consulting	Completed
2	Exec Office	Organizational Ethics/Culture	Consulting	In-Progress
3	Exec Office	LA County Rehired Retiree	Audit	Completed
4	Exec Office	Business Continuity Plan	Advisory	Q3
5	Organizational	Continuous Audit Processing (CAP)	Audit	Continuous
6	Organizational	Recommendation Follow-Up	Other Projects	Continuous
7	Organizational	Risk Assessment	Other Projects	Continuous
ADMINISTRATION - Admin Services, HR, Systems				
8	Systems	IT Risk Assessment	Audit	Q4
9	Admin/Systems	Inventory Asset Management	Audit	Q3
10	Admin Services	Procurement of Goods	Audit	Completed
11	HR	LACERA Rehired Retirees	Audit	In-Progress
12	Systems	Oversight of SOC Audits FYE 23 & 24	Oversight	Continuous
13	HR	Follow-up Assessment of Recruitment & Hiring	Audit	In-Progress
INVESTMENTS & FASD				
14	FASD	Wire Transfers (BofA)	Audit	Completed
15	FASD	CEO Credit Card	Audit	Completed
16	FASD	Oversight of Financial Audit FYE 23 & 24	Oversight	Continuous
17	Investments	RFP - Actuarial Services	Advisory	In-Progress
18	Investments	Oversight of Actuarial Audit FYE 23 & 24	Oversight	Continuous
19	Investments	Oversight THC Financial Audits - FYE 23 & 24	Oversight	Continuous
OPERATIONS - Benefits, DRS, RHC, Member Services				
20	Benefits	Account Settlement Collections (Overpayments)	Advisory	Q4
21	Benefits	LA County Payroll	Audit	Q4
INTERNAL AUDIT OPERATIONS				
22	Internal Audit	RFP - Audit Committee Consultant	Other Projects	Completed
23	Internal Audit	Professional Development / CPE	Other Projects	Continuous
24	Internal Audit	Quality Assurance Improvement Program	Other Projects	Continuous
25	Internal Audit	Audit Committee Support	Other Projects	Continuous
ADDED PROJECTS				
26	Benefits	Replacement Plan 415B	Addition	Completed
27	FASD	Internal Controls over Financial Reporting	Addition	Completed
28	HR / Systems	Termination Of Access	Addition	Q4
29	Exec Office	External Audit of OneMeeting (Net Force)	Addition	Completed

# **Fiscal Year End 2024 Internal Audit Plan Status Report**

**(as of March 5, 2024)**

---

Presented by:

Nathan Amick, Senior Internal Auditor



# Recently Completed Audit Projects & Engagements

(since November 30, 2023)

Completed Since Last Audit Committee Meeting	Project Type	Report Date
External Audit of OneMeeting (Net Force)	Audit	December 11, 2023
RFP - Audit Committee Consultant *	Advisory	N/A
Bank of America Wire Transfer Audit	Audit	March 5, 2023
Procurement of Goods	Audit	March 5, 2023

\* At the December 2023 Audit Committee, The Committee selected Larry Jensen to be their Audit Committee Consultant. A contract with Mr. Jensen was finalized on February 1, 2024.

# Continuous and Current Audit Engagements



The projects below (10) are perpetual, and the work is up to date as of March 5, 2023. All projects will be completed June 30, 2024, and will recommence July 1, 2024 for FYE 2025. Projects with an asterisk (\*) are Internal Audit administrative responsibilities.

## Continuous Audit Engagements/Projects

Continuous Audit Processing (CAP)

Oversight of Actuarial Audit FYE 23 & 24

Oversight of Financial Audit FYE 23 & 24

Oversight of SOC Audits FYE 23 & 24

Oversight THC Financial Audits - FYE 23 & 24

Professional Development / CPE\*

Quality Assurance Improvement Program\*

Recommendation Follow-Up\*

Risk Assessment\*

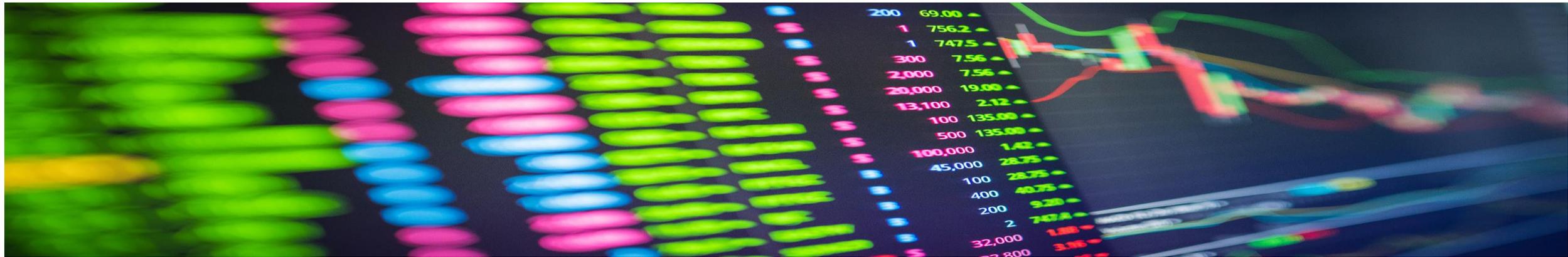
Audit Committee Support\*



# In Progress Audit Engagements & Projects as of March 5, 2024



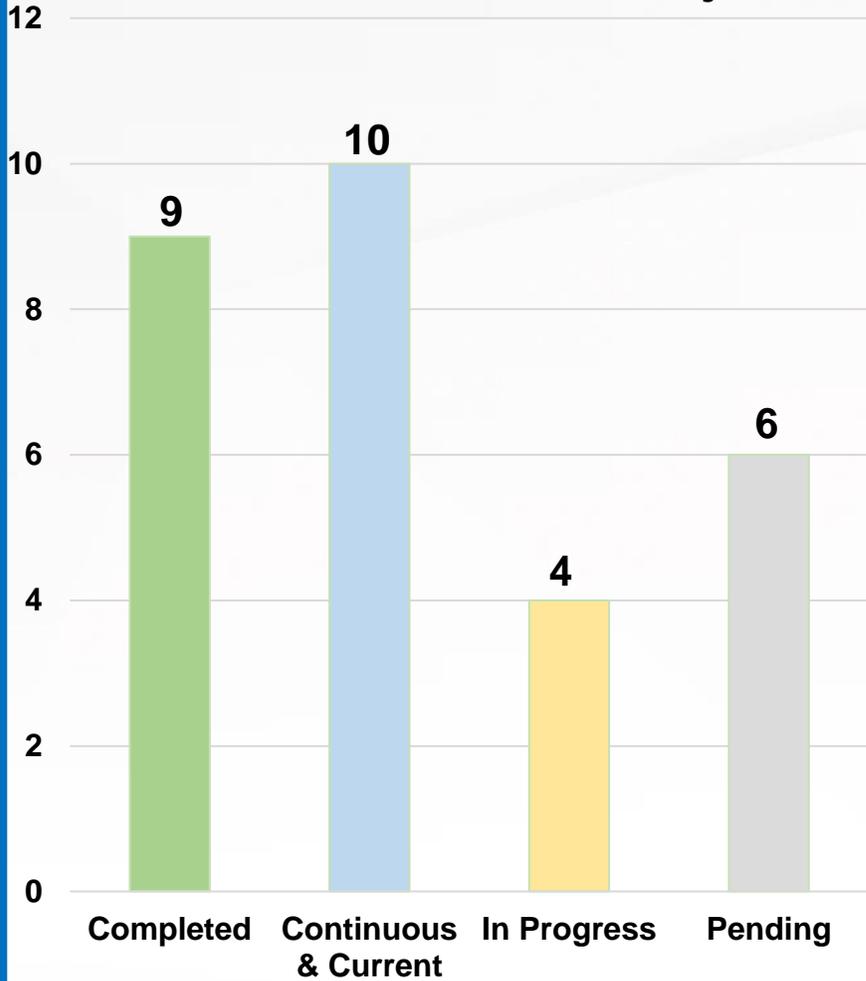
In Progress - Engagement/Project	Engagement Assignment	Estimated Completion	Planning Scope	Prelim Audit Work	Audit Field Work	Draft Report	Exit Meeting
RFP Actuarial Services	Investments & Internal Audit	May 2024	n/a	n/a	n/a	n/a	n/a
Organizational Ethics/Culture	Internal Audit	June 2024					
LACERA Rehired Retirees	Internal Audit	June 2024					
Follow-up Assessment of Recruitment and Hiring	Internal Audit	April 2024					



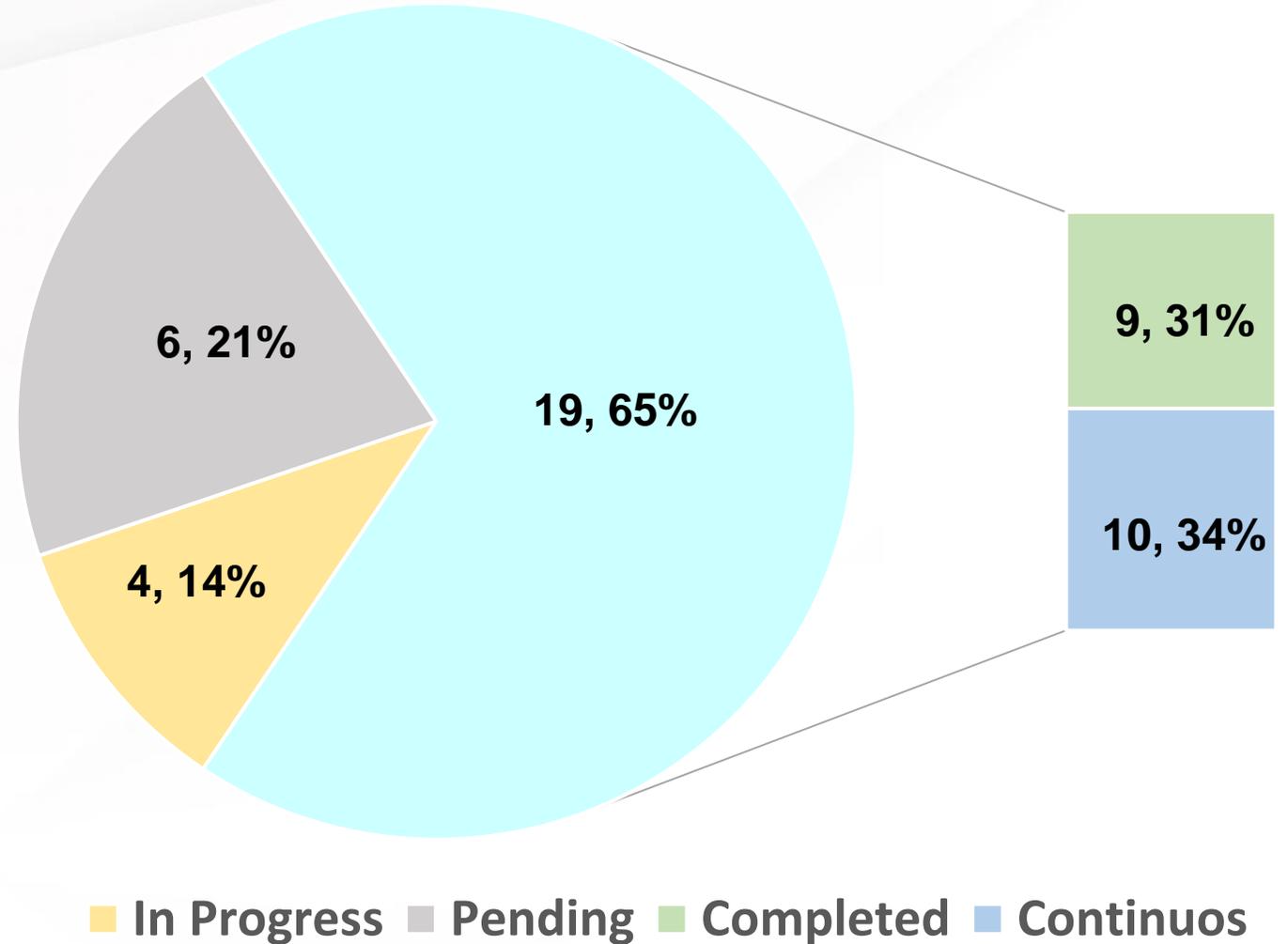
# FYE 2024 Audit Project Dashboard



### Status of Audits and Projects



### Percentage of Completion – 29 Projects



# Pending Audit Engagements & Projects



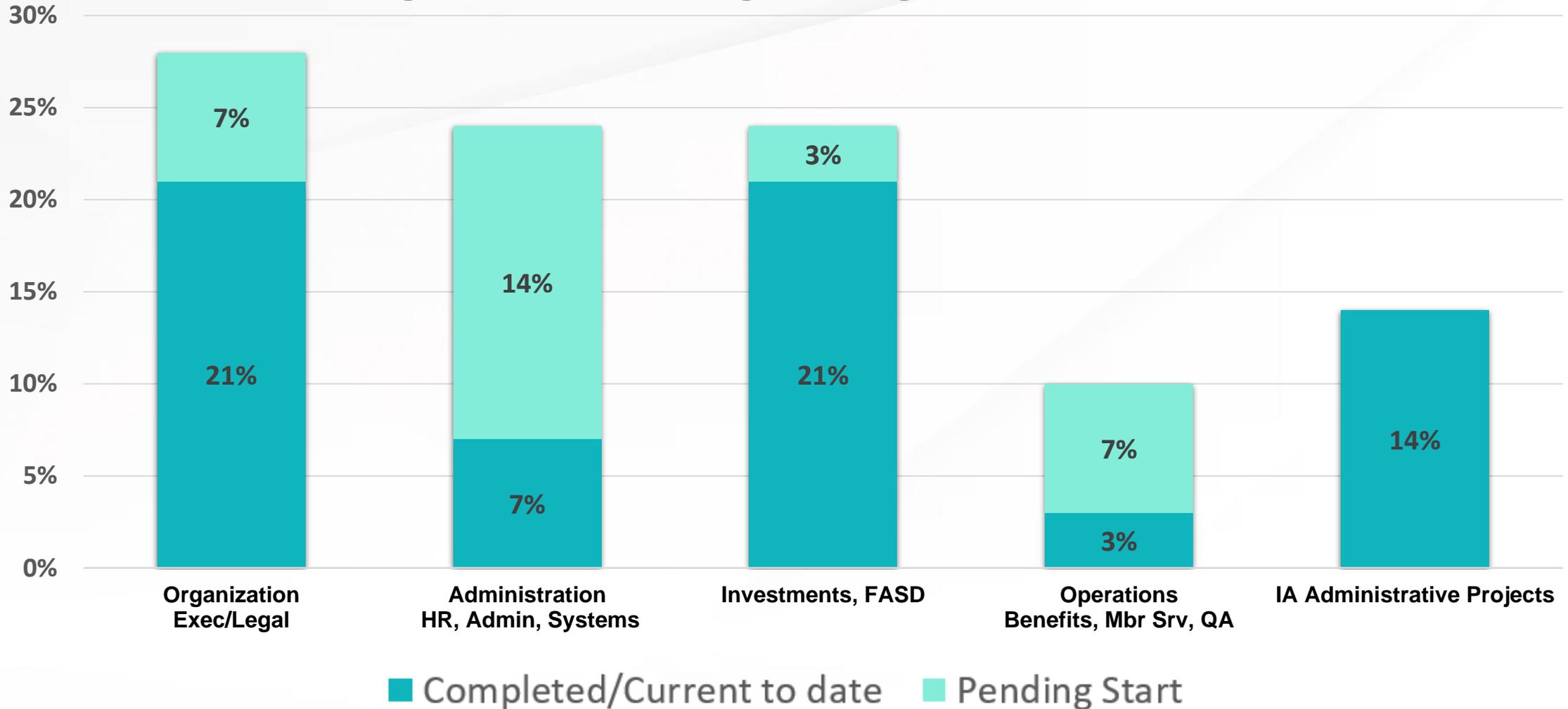
As of March 5, 2024, Internal Audit has yet to begin work on these FYE 2024 Audit Plan projects.

Pending Engagement/Project	Audit Assignment	Estimated Start
Business Continuity Plan	Internal Audit	Quarter 3
Inventory Asset Management	External	Quarter 3
IT Risk Assessment	External	Quarter 4
LA County Payroll	Internal Audit	Quarter 4
Termination Of Access	Internal Audit	Quarter 4
Account Settlement Collections (Overpayments)	Internal Audit	Quarter 4

# FYE 2024 Audit Project Dashboard



## Audit Plan Coverage Allocated Throughout Organization



# Progress Implementing IA Recommendations



23 Recommendations were issued from our External Quality Assessment in March 2022

- 8 recommendations were implemented
- 15 recommendations remain open
  - Prioritized 7 foundational recommendations

New Global Internal Audit Standards issued in January 2024

- Conducting a self-assessment of Internal Audit's readiness for the new standards to determining if the recommendations are still applicable. ETA October 2024





March 4, 2024

TO: Each Trustee,  
Audit Committee

FROM: Santos H. Kreimann, <sup>SHK</sup>  
Chief Executive Officer

Luis A. Lugo <sup>LL</sup>  
Deputy Chief Executive Officer

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Management's Compliance Report**

As required in Section VII.E.4 of the 2021 Audit Committee Charter, Management provides this memo to summarize its compliance efforts during the past year.

## **A. LACERA Ethics and Compliance Program**

### *1. 2023-2028 Strategic Plan*

The goal of Strategic Objective 4.1 of LACERA's 2023-2028 Strategic Plan, adopted by the Board of Retirement in July 2023, is to develop and implement an enterprise Ethics and Compliance Program (Program) as an element of a mature organizational risk governance structure. Currently, LACERA does not have a formal, centralized Program, but rather an organization-wide Code of Ethical Conduct, Conflict of Interest Code, other related policies, and various divisions have compliance functions specific to their individual operations.

The purpose of a centralized Ethics and Compliance Program is to promote a framework within which Management, the Audit Committee, and the Boards may better exercise their duty of oversight and promote a strong, engaged culture of ethical conduct based on LACERA's Values, sound judgment, and compliance with laws, regulations, policies, and procedures.

An independent and objective Program will further LACERA's fiduciary duties of loyalty and prudence under the [California Constitution \(Article XVI, Section 17\)](#) and [CERL \(California Government Code Section 31595\)](#). LACERA's Program will follow best practices in the public pension industry and consistent with the U.S. Sentencing Commission's 1991 Sentencing Guidelines for Organizations, the Department of Justice's 2023 ["Evaluation of Corporate Compliance Programs"](#) guidance, and the Institute of Internal Auditor's 2020 [The Three Lines Model](#).

///

///

## *2. Status of Program Development*

Management and staff have, in consultation with ethics and compliance counsel, developed a proposed Program structure that follows the best practices listed above. The Program is described in a proposed Ethics and Compliance Program Charter which, thus far, has been presented to the Board of Retirement's Operations Oversight Committee, the Board of Retirement itself, and, most recently, the Joint Organizational Governance Committee (JOGC) at its February 29, 2024 meeting.

The JOGC recommended that the Board of Retirement and Board of Investments refer the proposed Program Charter to the Audit Committee for further development, ultimately to be returned to the full Boards for final approval. The JOGC's recommendation will be presented to the Boards at their respective April 2024 meetings, and assuming the JOGC's recommendation is approved, to the Audit Committee at its next meeting, currently scheduled for June 2024.

Management will not further describe the elements of the proposed Charter in this memo to preserve the integrity of the above-noted process approved by the JOGC.

### **B. Enterprise Risk Management**

The Board of Retirement's 2023-2028 Strategic Plan, Objective 4.2, also calls for development of an Enterprise Risk Management (ERM) program. The Internal Audit Division will take the lead on that program, working in conjunction with Management and other key staff. Management will report on the progress of the ERM Management program in future memos.

### **C. Staff Ethics and Compliance Committee**

The multi-divisional staff Policy Committee was formed in late 2021 and began meeting monthly in February 2022. After establishing a Committee Charter, a Policy Development Checklist, and updating LACERA's Policies on Policies, the Committee began inventorying policies and procedures organization-wide, reviewing policies and procedures due for scheduled review, reviewing newly proposed policies, and researching policy management software solutions to house LACERA's policies, procedures, and charters in a central, searchable, and functional location.

As of November 2023, the staff Policy Committee evolved into the Ethics and Compliance Committee (ECC), with the Committee Program Charter rewritten to reflect this evolution. Since Management's last compliance report (February 2023), the ECC has reviewed the following proposed policies and charters:

1. Privacy and Confidentiality Policy
2. Post Retirement Employment Policy

3. Reimbursement Election Submission Policy
4. Rock Solid: OneMeeting Application Policy
5. Accounts Payable Policy
6. Processing Internal Disability Retirement Applications and Appeals
7. Ethics and Compliance Committee Charter
8. Audit, Compliance, Risk, and Ethics (ACRE) Committee Charter
9. Revised AB 2449 Teleconference Policy
10. Non-LACERA Managed Devices and Acceptable Use Policy
11. Recovery of Member Overpayments and Underpayments
12. Ethics and Compliance Program Charter
13. Budget Policy
14. Secure Workplace Policy

#### **D. Governance, Risk, and Compliance Software**

Management and staff, working with the staff IT Coordinating Council and the staff Ethics and Compliance Committee, have devoted a concerted effort to development requirements for a suite of Governance, Risk, and Compliance (GRC) software to assist with organizational risk management. A full GRC solution will include separate modules for: 1) information security; 2) policy management; 3) ethics and compliance (including privacy); 4) audit; and 5) enterprise risk management.

Solution requirements will be completed in the coming months, after which, providers and products in the market will be researched, followed by an Invitation to Bid to select one or more vendors to provide the most comprehensive solution for the required five modules. As the procurement process moves forward, all necessary approvals will be obtained in accordance with the Board of Retirement's Purchasing Policy on Goods and Services.

#### **E. Information Security**

Information security continues to be enhanced under the leadership of the Information Security Officer (ISO). The ISO will separately report on his work.

#### **F. Contract Management Process**

The Administrative Services Division has undertaken a comprehensive review of procurement and contract processes to ensure compliance with the Purchasing Policy and best practices in third party risk management.

#### **G. Other Divisional Efforts**

Efforts are underway or planned throughout LACERA to focus on organizational compliance and enhancement of processes. Management recognizes that compliance is

Re: Management's Compliance Report

March 4, 2024

Page 4 of 4

a collaborative "whole organization" effort and actively discusses and promotes review of compliance processes in all divisions. These efforts will be reported as they progress.

#### **H. Conclusion**

Management welcomes the input of the Audit Committee with respect to Management's oversight of ethics and compliance.

c: Jonathan Grabel  
JJ Popowich  
Laura Guglielmo  
Steven P. Rice  
Richard Bendall  
Chaitanya Errande  
Ricki Contreras  
Kathy Delino  
Leisha Collins  
Christina Logan  
Celso Templo  
MAC Team

**FOR INFORMATION ONLY**

March 5, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Nathan K. Amick   
Senior Internal Auditor

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Recommendation Follow-Up Report**

**Background**

The Institute of Internal Auditors' (IIA) Performance Standard 2500 requires the Chief Audit Executive (CAE) to establish and maintain a follow-up process to monitor and ensure recommendations have been effectively implemented or that executive management has accepted the risk of not addressing the underlying finding of the recommendation.

**Internal Audit's Follow-Up Process**

During the audit process, Internal Audit may identify findings or make recommendations to address risks or improve a process. The responsible division manager and the Executive Office review the findings and recommendations. Subsequently, the division manager provides responses indicating how and when planned improvements will be made. The final audit report includes the audit findings, recommendations, management's responses, and targeted completion date. Internal Audit tracks recommendations through TeamMate+, our audit management software, and regularly follows up with Management. Internal Audit is responsible for 1) ensuring that Management's action plans have been effectively implemented, or 2) ensuring that Management remains aware of the risks that they accept by not taking action in a timely manner. On a quarterly basis, Internal Audit reports the status of all outstanding audit recommendations to the Audit Committee.

Recommendations are classified based on the responsible party's progress:

- **On Track** – The responsible party began implementing the recommendation and is currently on track to meet the target implementation due date. Management can extend the target implementation due date with the Executive Office's approval.

- **At Risk / Behind Schedule** – The responsible party has not made enough progress to implement the recommendation by the target implementation due date.
- **Implemented** – The responsible party provided documentation and the Internal Auditor verified the satisfactory implementation of the audit recommendation.
- **Overdue** – The responsible party has failed to implement the recommendation by the target implementation due date and has not completed the extension request.
- **Pending Internal Audit’s Verification** – The responsible party has stated and provided support they addressed the recommendation, but Internal Audit has not yet verified the implementation. Internal Audit does not close out a recommendation without completing an internal verification procedure.

**Monitoring and Reporting for Fiscal Year 2024** As result of the audit and consulting projects completed in the recent months, Internal Audit is tracking both audit recommendations and long-term strategic recommendations. Audit recommendations are focused on improving internal controls while strategic recommendations are centered on organizational risks that may impact LACERA in the future. The reporting period is from November 16, 2023 through February 29, 2024. Audit reports and recommendations released after February 29, 2024, will be included in the next quarterly reporting to the Audit Committee.

	# of Audit Recommendations	# of Strategic Recommendations
<b>Balance as of 11/16/2023</b>	<b>24</b>	<b>15</b>
+ New Findings	0	0
- Accepts Risk	0	0
-Pending Internal Audit Verification	-10	0
- Implemented Findings	-4	0
<b>Balance as of 02/29/2024</b>	<b>10</b>	<b>15</b>

Included in this memo are the following attachments for the Audit Committee to review:

- Attachment A – Presentation of outstanding audit recommendations and long-term strategic recommendations for the period from November 16, 2023 through February 29, 2024.
- Attachment B – Details of outstanding audit recommendations as of February 29, 2024.
- Attachment C – Details of outstanding long-term strategic recommendations as of February 29, 2024.

Staff from the respective divisions will be present at the March 2024 Audit Committee meeting to address any questions.

Noted and Reviewed:  
  
 Richard P. Bendall  
 Chief Audit Executive



ATTACHMENT A

# Recommendation Follow-Up Progress

(As Of February 29, 2024)

---

Presented by:

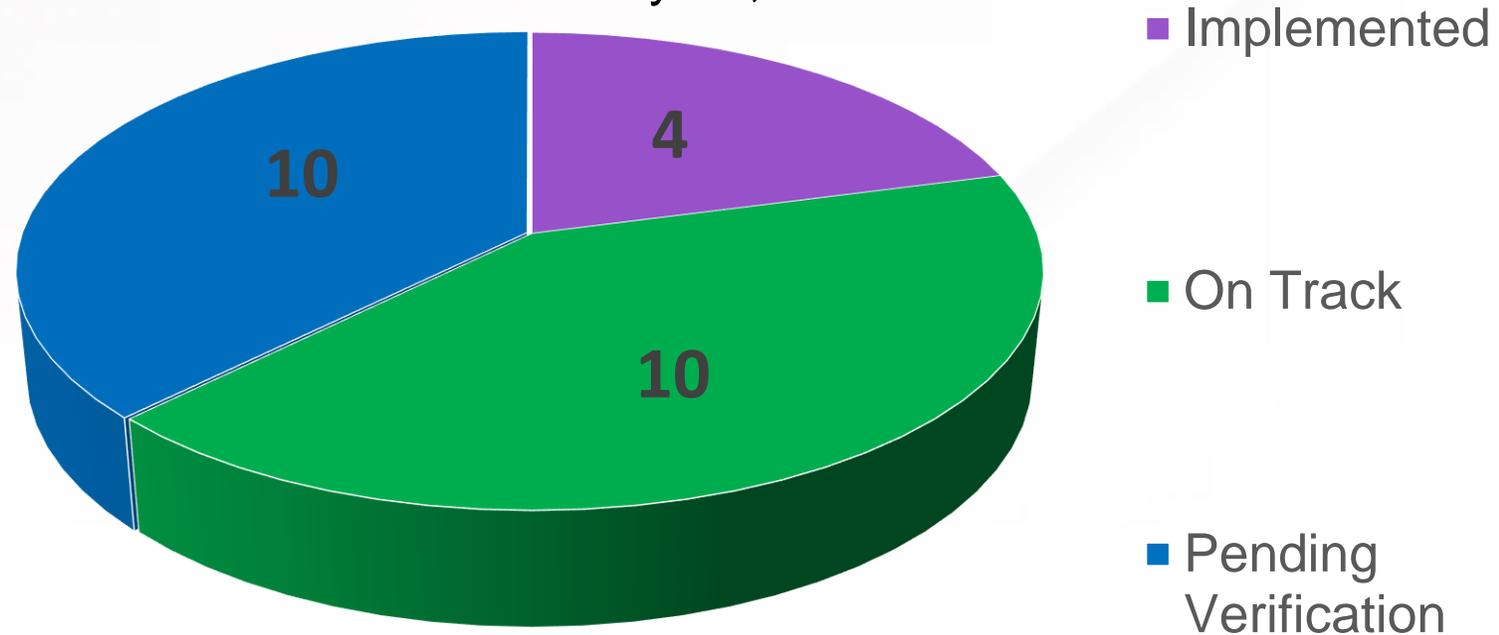
Nathan K. Amick, Senior Internal Auditor

# Status of Open Audit Recommendations



Outstanding audit recommendations are classified based on the responsible party's progress and assigned categories based on the fundamental intent of the recommendation. The reporting period is from November 16, 2023 to February 29, 2024. Audit reports and recommendations released after February 29, 2024 will be included in the next quarterly reporting to the Audit Committee.

Status of Outstanding Audit Recommendations  
as of February 29, 2024



# Status of Open Audit Recommendations



Audit recommendations address operational risks and focus on improving internal controls. These recommendations are directed towards specific divisions within the organization. In some cases, implementation requires extensive coordination between multiple divisions. Table below illustrates the outstanding audit recommendations by divisions.

## Open Audit Recommendation By Divisions

Division	Implemented	On Track	Pending Internal Audit's Verification
Administrative Services Division	-	1	-
Disability Retirement Services Division (DRS)	1	1	-
Financial Accounting & Services Division (FASD)	1	5	-
Human Resources Division (HR)	-	2	9
Information Security Office	2	1	1
<b>Total</b>	<b>4</b>	<b>10</b>	<b>10</b>

# Status of Open Strategic Recommendations



Strategic recommendations cover the broader operating risks and control gaps that require attention from the Executive Office. Executive Office is addressing many of these recommendations through LACERA's Strategic Plan FYE 2023-2028. Internal Audit last conducted its annual in-depth assessment of these recommendations in August 2023.

## Recommendations to be evaluated as part of FY23-24 strategic planning

Strategic COSO* Area	# of Recos
Organizational Structure	3
Internal and External Reporting	1
Forecasting/Budget	1
Risk Assessment	1
Training and Development & Talent Management	7
Performance Measures	2
<b>Total</b>	<b>15</b>

\* Internal Audit aligned these Strategic Recommendations against COSO's Internal Control Framework as many of these recommendations relate to broad organizational level controls described in the Framework. *COSO refers to the internal control framework developed by the Committee of Sponsoring Organizations of the Treadway Commission.*

### Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Administrative Services Division</b>					
Audit of Contract Operations (Procurement of Services)	2019 Policy and 2020 Manual are past review dates	Medium	Administrative Services Division Management should review and update the 2019 Policy for Purchasing Goods and Services and 2020 Purchasing and Contract Administration Manual accordingly.	<b>ON TRACK - 2nd Approved Extension.</b> This recommendation will also, be incorporated into the Procurement of Goods Audit.	6/30/2024

Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Disability Retirement Division (DRS)</b>					
Audit of Disability Retirement Business Process	A mechanism to identify affiliated disability applicants does not exist.	Medium	DRS Management should develop a formal control mechanism for identifying disability applicants affiliated with LACERA employees or the Board of Retirement.	<b>ON TRACK - 2nd Approved Extension.</b> DRS was advised by legal counsel to make no changes to the applications until LACERA Policy For Processing Disability Retirement Applications and Appeal Filed by Internal and Internal Related Applicants (approved by BOR in December 2023).	3/31/2024
Audit of Disability Retirement Business Process	The current practices for processing affiliated disability applications are not documented in a formal policy.	Medium	DRS Management and LACERA's Legal Office should update its Policy to include current practices for processing disability applicants affiliated with LACERA employees or the BOR. A formal documented Policy will help prevent staff from processing affiliated applications that require outsourcing to third-party investigators.	<b>IMPLEMENTED</b> - The policy was presented at the December 6, 2023 Board of Retirement meeting. The updated policy is now reflected on LACERA.com.	-

**Operational Recommendation Follow-Up Report**

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Financial and Accounting Services Division (FASD)</b>					
Audit of Wire Transfers - State Street (R/F from FYE 2022)	Cash Manager authorize divisional representative lists are outdated.	Low	FASD management should review and update the authorized divisional representative lists at least biennially.	<b>IMPLEMENTED</b> - FASD will maintain the accuracy of the divisional lists on an ongoing basis, whenever staffing changes occur. This will be included in our future periodic CAP tests of controls around wire transfers.	-
Audit of Corporate Credit Cards	1 - The Corporate Credit Card Policy has not been updated to reflect current practices.	Medium	1. FASD Management should update LACERA's Corporate Credit Card Policy. The Policy should include the date of next review in accordance with LACERA's requirements.	<b>ON TRACK - 2nd Approved Extension.</b> Delays in providing updates to the Policy due to immediate competing projects. The revised Policy will include updates to strengthen procedural tasks as noted.	6/30/2024
Audit of Corporate Credit Cards	1 - The Corporate Credit Card Policy has not been updated to reflect current practices.	Medium	2. FASD Management should provide training on the new policy and requirements to all cardholders and division secretaries.	<b>ON TRACK - 1st Approved Extension.</b> There are currently delays in providing updates to the Policy due to immediate competing projects. Training will be provided when updates to the policy are completed.	6/30/2024

**Operational Recommendation Follow-Up Report**

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Financial and Accounting Services Division (FASD)</b>					
Audit of Corporate Credit Cards	2 - Missing and untimely reporting of supporting documentation for credit card transactions.	High	4. FASD Management should provide training to staff once the Policy is revised to ensure that staff are aware of requirements and expectations for supporting documentation.	<b>ON TRACK - 1st Approved Extension.</b> There are currently delays in providing updates to the Policy due to immediate competing projects. Training will be provided when updates to the policy are completed.	6/30/2024
Audit of Corporate Credit Cards	3 - There is no formal process for the identification and subsequent de-activation of credit cardholders that have terminated employment or transferred to a new position.	High	5. FASD Management should ensure that the Policy and/or procedures incorporate controls to ensure the timely notification to FASD of changes in the employment status of a cardholder.	<b>ON TRACK - 2nd Approved Extension.</b> FASD now receives HR outgoing staff emails to deactivate accounts and destroy credit cards for outgoing staff. These new procedures be updated in the Policy which is delayed.	6/30/2024

### Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
Audit of Corporate Credit Cards	3 - There is no formal process for the identification and subsequent de-activation of credit cardholders that have terminated employment or transferred to a new position.	High	6. FASD Management should ensure that the Policy and/or procedures require FASD staff to deactivate the cards and associated access to the banking application.	<b>ON TRACK - 2nd Approved Extension.</b> FASD is also working on receiving notifications from HR for LACERA staff members that are transferred between divisions.	6/30/2024

**Operational Recommendation Follow-Up Report**

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Human Resources Division (HR)</b>					
Review of HR Recruiting & Hiring Process	#3: Lack Structure, Culture & Service Level Agreements	N/A	HR should perform a needs assessment to determine whether additional resources are needed by performing the following activities: i.) an evaluation of the competencies of the team; ii.) performing a skills and capabilities assessment; iii.) identifying areas of strengths and professional development needs; iv.) an analysis of the division's tasks performed; and v.) the associated time requirements.	<b>On Track - Approved 2nd Extension.</b> IA reviewed the SOW for the needs assessment with HR and AEO that will be distributed in April 2024 after one additional new HR staff is onboarded.	6/30/2024

**Operational Recommendation Follow-Up Report**

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
LA County Rehired Retirees FYE 2021	Spike in the number of Rehired Retirees Exceeding 960-Hour Limit	High	<p>1. We recommend LACERA's CEO formally request the County CEO in conjunction with the County Director of Human Resources and Auditor-Controller to prepare a corrective action plan that consolidates and actively monitors the rehired retiree (960- hour limit) reporting requirements for all County departments.</p> <p>2. We recommend LACERA's Executive Office, Systems, and Benefits work with the County's CEO Office and Auditor-Controller to establish an automated feed of rehired retirees' hours as part of payroll data.</p> <p>3. We recommend LACERA's Executive Office, Legal Office, and</p>	<p><b>PENDING INTERNAL AUDIT VERIFICATION -</b> The FYE 2023 iteration of this audit was performed. Based on the 960 test work in that audit, we have determined the recommendation implemented.</p>	6/30/2024

## Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Human Resources Division (HR)</b>					
LA County Rehired Retirees FYE 2021	Lack of adherence to PEPRA's "limited duration" language	High	We recommend LACERA's Executive Office and Legal Office work with the Board of Retirement to determine a more defined "bright-line" definition of limited duration to ensure compliance with PEPRA and provide for recovery of benefits paid during periods worked in violation of PEPRA law.	<b>On Track - 2ND Approved Extension.</b> Chief Legal Council has not had time to advance discussions with The County and believes that the end of FYE 2024 is a more realistic implementation date.	6/30/2024
LACERA Rehired Retirees Audit	#1 - Lack of Ensuring Compliance in the Administration of The Rehired Retiree Program	High	LACERA's Executive Office and HR should meet and confer around the expectations for compliance with the Post Employment Rehired Retiree Policy. HR should then revise their procedure accordingly.	<b>PENDING INTERNAL AUDIT VERIFICATION -</b> In July of 2023, The BOR approved the updated Post Employment Retirement Policy, setting compliance standards for the program.	12/31/2023
LACERA Rehired Retirees Audit	#1 - Lack of Ensuring Compliance in the Administration of The Rehired Retiree Program	High	HR Management ensure 960 Request Forms are completed and approved by the Executive Office, and all required documentation is obtained each fiscal year prior to the rehired retiree beginning work.	<b>PENDING INTERNAL AUDIT VERIFICATION -</b> Reviewed all four RR, "Request For Employment Of Retiree" forms for FYE 2024 (through 1/15/2024) without exception.	12/31/2023

### Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
LACERA Rehired Retirees Audit	#1 - Lack of Ensuring Compliance in the Administration of The Rehired Retiree Program	High	HR Management to ensure that missing documentations identified in this audit are obtained for the rehired retirees that worked in FY 2020-2021.	<b>PENDING INTERNAL AUDIT VERIFICATION -</b> Where feasible HR management obtained the missing documentation. When not feasible HR management provided written justification as to why.	11/27/2023

## Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Human Resources Division (HR)</b>					
LACERA Rehired Retirees Audit	#3 - Lack of Specific Limits in Defining Limited Duration	High	LACERA Executive Management should develop an expedited plan to transition from the retiree to permanent staff and report that plan to the Board of Retirement.	<b>PENDING INTERNAL AUDIT VERIFICATION -</b> The updated Post Employment Retirement Policy, includes requiring a "description of the plan to complete the retiree's work or transition it to a current staff member" when requesting approval for rehired retiree.	11/27/2023
Audit of LACERA Rehired Retirees for FYE June 30, 2022	Continued Lack of Compliance in the Administration of The Rehired Retiree Program	High	4.HR Management monitor compliance with the new 2023 Policy to ensure that rehired retirees only work the period approved to work.	<b>PENDING INTERNAL AUDIT VERIFICATION -</b> Tested current rehired retirees and verified work hours were being captured in WorkSpace, and obtained sample copy of template for LACERA communication with retiree regarding limiting work hours to 960.	12/31/2023
Audit of LACERA Rehired Retirees for FYE June 30, 2022	Continued Lack of Compliance in the Administration of The Rehired Retiree Program	High	5. HR Management ensure that rehired retirees are compensated at the rate of pay that is commensurate with what LACERA pays to staff performing comparable duties.	<b>PENDING INTERNAL AUDIT VERIFICATION -</b> The FYE 2023 iteration of this audit was performed. Based on the compensation test work in that audit, we have determined the recommendation implemented.	12/31/2023

Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
Audit of LACERA Rehired Retirees for FYE June 30, 2022	Continued Lack of Compliance in the Administration of The Rehired Retiree Program	High	6. For the overpayment identified, calculate the total amount overpaid and facilitate the collection of the overpayment.	<b>PENDING INTERNAL AUDIT VERIFICATION -</b> Collection of overpayments has been set up through Benefits from the member's monthly retirement payment.	12/31/2023
Audit of LACERA Rehired Retirees for FYE June 30, 2022	Continued Lack of Specific Limits in defining "limited duration"	High	10. In the case that supports the need to deviate from the policy, HR Management should ensure that, at a minimum, the justification is documented and approved by the CEO on the Request.	<b>PENDING INTERNAL AUDIT VERIFICATION -</b> In June of 2023, The BOR approved the updated Post Employment Retirement Policy, setting compliance standards for the program.	12/31/2023

**Operational Recommendation Follow-Up Report**

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Information Security</b>					
Board Vantage Security Settings	Expected application access control restrictions were not validated	High	LACERA's Information Security Office should require and ensure that appropriate and available audit trails are built and/turned on, and periodically reviewed for all LACERA [OneMeeting] applications.	<b>On Track - 2nd Approved Extension.</b> The Information Security Office is finalizing its policy on audit trails as part of its WISP (written information security program). Subsequent to the policy being finalized, the Project Management Office will assess internal and external applications' audit logs for compliance with the policy.	6/30/2024
Board Vantage Security Settings	Support Application Audit Trails and Restrictions were Deficient	High	<ol style="list-style-type: none"> <li>1. LACERA should ensure that audit logs from OneMeeting and BoardVantage includes key data to run reports based on user, document, and log-on activities.</li> <li>2. LACERA's Executive Office should establish and conduct periodic reviews of audit log reports for user, document, and log-on activities.</li> <li>3. LACERA's Executive Office should consistently monitor unauthorized access or inappropriate access to documents.</li> </ol> [REVISED Nov '23]	<b>IMPLEMENTED -</b> Support applications no longer in use.	-

### Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
Third-Party Data Security	Finding #1 Inadequate communication regarding non-compliance with vendor contracts	High	Administrative Services should build into its control process additional warnings to Contract Administrators, escalating non-compliance to the Executive Office, and implementing consequences, like stopping payments for vendors with non-compliance contracts.	<b>PENDING INTERNAL AUDIT VERIFICATION</b> - Per contract management system administrator; current CMS is sending notices to contract owners & administrators, additional staff have been hired to focus on contract issues as they arise. Also, user training has begun on the new ECLM contract system which includes additional compliance control warnings.	2/5/2024

### Operational Recommendation Follow-Up Report

Project Name	Finding Title	Risk Rating	Recommendation	Status Update	Target Due Date
<b>Responsible Division: Information Security</b>					
Third-Party Data Security	Finding #2 No formal procedures for review of vendor security reports	Low	InfoSec management should document its review when approving vendor security reports. The documentation should include a checklist of key areas reviewed and any additional research and communications needed to obtain adequate assurance about the vendor's security posture.	<b>IMPLEMENTED-</b> Infosec has created necessary document review checklist.	-

## Strategic Recommendation Follow-Up Report

Project Name	Finding Title	Recommendation	Status Update
<b>COSO: Forecasting / Budgeting</b>			
Risk & Controls Assessment - Retiree Healthcare	OBS 4 - RHC's administrative fee process is not formalized.	N/A - This was a strategic observation made by Internal Audit.	The Executive Team has already met with LA County's CEO and agreed on a process for tracking, monitoring, and reporting on RHC's administrative fee. The Executive Office needs to draft a Memo of Understanding (MOU) to formalize the process.
<b>COSO: Internal &amp; External Reporting</b>			
Organizational Governance Review	OBS 7 - LACERA does not have a communication plan	LACERA should finalize the existing draft Communication Plan for the organization. In addition, guidelines for style and format of reporting should be developed to ensure consistency. Staff should be trained on the implemented Communication Plan and style and format guidelines.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 1st objective, "Superior Member Experience."
<b>COSO: Organizational Tone</b>			
Quality Assurance Operations Review	Finding #1 - The QA Division's independence is weakened when reporting to the same AEO over the operational areas in which they perform quality assurance audits.	LACERA Executive Management should work with QA and the MOG Divisions to develop a plan and timeline for a) relocating training and metrics out of the QA Division to an operational division, and b) changing the reporting structure such that the QA Division reports independently to the Administrative AEO.	The Executive Team and HR are working together to address this in the long-term as this requires a significant amount of resource planning and strategizing within the organization.
Organizational Governance Review	OBS 5 - The LACERA CEO job description and the responsibilities of the Board Committees overlap/conflict	The BOR's Committee Charters and the Chief Executive Officer's (CEO) job description should be reviewed and updated to reflect the appropriate responsibilities of each. The Charters should include oversight responsibilities while the CEO job description should include responsibilities for carrying out the Board directives and management of the organization.	The Executive Team and Board Leadership are actively working to address this recommendation both through the Strategic Plan.

**Strategic Recommendation Follow-Up Report  
As of August 2023**

Organizational Governance Review	OBS 6 - LACERA does not have a formal enterprise fraud prevention and detection program	LACERA should implement a formal fraud prevention and detection program that includes a policy separate from the Ethics Policy, consistent training for staff including how to report suspected fraud, and a process to incorporate what is learned from the fraud reporting into the organization's policies.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 4th Objective "Enterprise Risk Management and Compliance."
----------------------------------	---	--	--

**COSO: Performance Measures**

Quality Assurance Operations Review	Finding #6: QA management does not have an annual quality assurance audit plan and does not have metrics and KPIs for managing their staff's work.	QA management should develop an annual quality assurance audit plan and key performance indicators (KPIs) to allocate and monitor QA staff resources.	To be evaluated as part of FY23-24 strategic planning
Organizational Governance Review	OBS 8 - LACERA lacks defined Key Performance Indicators (KPI)	LACERA should develop and implement key performance indicators (KPI's) for any divisions that have not yet defined them. The KPI's should be quantifiable and be linked to the goals of the organization as established in the Strategic Plan (see Obs-01). In addition, reporting mechanisms should be established for the reporting of the KPI's so that the data can be used to inform decision making.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 5th objective, "Fiscal Durability."

**COSO: Risk Assessment**

Organizational Governance Review	OBS 9 - LACERA does not have a formal enterprise risk management and compliance program	LACERA should implement a formal enterprise risk management and compliance program for the organization that includes identification of risks and how to address those risks. The risk information should be used by the organization to make decisions. The program should also include an inventory of all program requirements and a plan to monitor compliance with those requirements. Reporting mechanisms should be implemented for risk management and compliance.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 4th Objective "Enterprise Risk Management and Compliance."
----------------------------------	---	--	--

**Strategic Recommendation Follow-Up Report  
As of August 2023**

**COSO: Training and Development & Talent Management**

Organizational Governance Review	OBS 3 - LACERA has not implemented a professional development plan	LACERA executive leadership should engage in a facilitated analysis of employees across the organization and identify specific development needs of employee classifications and functional groups.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 3rd Objective "Investing in People."
Organizational Governance Review	OBS 4 - LACERA does not have a succession plan	LACERA should implement a succession planning process to ensure that the organization can maintain a workforce that collectively possesses the core competencies and skills needed to accomplish its strategic objectives. Effective succession planning focuses on current and future needs and develops a pool of high potential personnel to meet the organization's long-term mission.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 3rd Objective "Investing in People."
Review of HR Recruiting & Hiring Process	#1: Lack a Planned, Measured and Optimized Recruiting Approach	1.a. LACERA's Executive Team should work with HR Management to develop an effective Workforce Plan and Implementation Strategies that clearly align with the organization's current and future Strategic Plans related to recruitment efforts.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 3rd Objective "Investing in People."
Review of HR Recruiting & Hiring Process	#1: Lack a Planned, Measured and Optimized Recruiting Approach	Identify an individual or committee (governance structure) to oversee the alignment of the approved Workforce Plan and HR's Implementation Strategies for recruiting.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 3rd Objective "Investing in People."
Review of HR Recruiting & Hiring Process	#1: Lack a Planned, Measured and Optimized Recruiting Approach	LACERA's Workforce Plan should address succession planning as a key component. Each division should perform forecasting of future vacancies through retirement and attrition. Succession candidates should be identified in each division and professional development should occur to prepare these members for future roles. We recommend that LACERA identify a Workforce Planning Model such as that established by the California Department of Human Resources or an alternative model.	This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 3rd Objective "Investing in People."

**Strategic Recommendation Follow-Up Report  
As of August 2023**

<p>Review of HR Recruiting &amp; Hiring Process</p>	<p>#3: Lack Structure, Culture &amp; Service Level Agreements</p>	<p>Based on the anecdotal evidence shared throughout this engagement it is apparent that LACERA's workplace culture is being affected in negative ways through perceptions and experiences of individuals who are directly related to the recruiting efforts, primarily at the Division level. As such, LACERA should perform an assessment of their HR Division to evaluate the team-member cohesiveness, related to employee satisfaction, level of engagement, perception of HR division management, and alignment with organizational strategy.</p>	<p>This recommendation will be considered as part of the work program for the Board of Retirement's 5-Year Strategic Plan (FY 2024-2029)'s 3rd Objective "Investing in People."</p>
<p>Risk &amp; Controls Assessment - Retiree Healthcare</p>	<p>OBS 2 - RHC is lacking succession planning between the management team and staff. RHC management has continued to rehire a retiree for over ten years</p>	<p>N/A - This was a strategic observation made by Internal Audit.</p>	<p>The OOC approved the LACERA Rehired Retiree policy which clarifies the associated requirements related to hiring rehired retirees, including ensuring a transition plan is established and followed.</p>

**FOR INFORMATION ONLY**

March 6, 2024

TO: 2024 Audit Committee  
Nancy Durazo, BOR Trustee  
Vivian Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Gabriel Tafoya   
Senior Internal Auditor

FOR: March 18, 2024, Audit Committee Meeting

**SUBJECT: Recommendation Follow-Up for Sensitive Information Technology Areas**

Internal Audit reports to the Audit Committee a summary of recently implemented and outstanding recommendations related to system and network security audits and assessments. This summary ensures the Committee remains informed about security measures and ongoing improvements. Our most recent addition is SOC 1 Type 2 Plante Moran audit FYE 2023, which is the first line in Table 1.

Table 1 summarizes the status of recommendations related to eight sensitive information technology (IT) engagements and one category of recommendations in which we previously consolidated duplicated recommendations. Nine (9) recommendations were implemented during this reporting period, November 2023 through February 2024. Table 2 summarizes the currently outstanding fourteen (14) recommendations by the different IT general controls areas.

**SUMMARY OF OPEN RECOMMENDATIONS**

**Table 1: Recommendations Status – By Audit Engagement**

Engagement Name Report Date	Total Recos	Implemented During Prior Periods	Implemented Nov 2023 – Feb 2024	In Progress Mar 2024
Recommendation Status by Risk Level				
<b>PM SOC FYE 2023</b> June 2023				
Medium	5	—	4	1
<b>PM SOC FYE 2022</b> June 2022				
Medium	5	4	1	—
<b>Moss Adams Pen and Social Engineering</b> April 2022				
High	3	2	1	—
Medium	3	2	—	1
Low	1	—	1	—
<b>PM SOC FYE2021</b> September 2021				
Medium	5	4	1	—
<b>PM SOC Readiness Assessment</b> February 2020				
Medium	10	9	—	1
<b>Clear Skies Penetration Test and VeraCode Report</b> March 2020				
High	1	1	—	—
Medium	25	21	—	4
Low	17	12	—	5
<b>Tevora 2019 Penetration Test</b> June 2019				
Low	5	4	1	—
<b>Tevora 2018 Security Risk Assessment</b> July 2018				
Medium	3	3	—	—
Low	6	5	—	1
<b>Consolidated Recos</b> January 2021				
High	2	2	—	—
Medium	2	1	—	1
<b>Totals</b>	<b>93</b>	<b>70</b>	<b>9</b>	<b>14</b>

For the reporting period ended February 2024, the following nine (9) recommendations have been implemented:

- The Human Resources Division and the Information Security Office (ISO) have addressed two recommendations from the PM SOC FYE 2023 audit. They implemented enhanced controls that address 1) the completion of security awareness training within 30 days of hire, and 2) acknowledgment of the security policies within 30 days of hire.
- The Systems Division (Systems) has addressed two recommendations from the PM SOC FYE 2023 audit. It provided training to its administrators on how to monitor and properly document the monitoring of various backup and security tools.
- Systems has addressed one recommendation from the PM SOC FYE 2021 audit. They implemented enhanced controls around keycard access.
- Systems has addressed one recommendation from the PM SOC FYE 2021 related to its servers.
- The Administrative Services Division and Systems have addressed the last high-risk recommendation from the Moss Adams' Penetration and Social Engineering audit. They updated physical security standards and training requirements for employees as well as notified staff of the various vectors and tactics that can be used by malicious persons that try to gain physical access to LACERA property, through both email (Security Safety Reminders) and Brown Bag meetings.
- Systems has updated its script library to address the one recommendation from the Moss Adams Penetration and Social Engineering Audit.
- Systems has addressed one recommendation from the Tavora 2019 Penetration Test. It updated all network devices authentication protocols.

For recommendations which are listed as **In Progress**, the Systems Division, and Information Security provided a summary of work to be performed and a timeline for completion.

## **RECOMMENDATIONS CATEGORIZED**

IT General Controls (ITGC) are the basic controls that can be applied to IT systems such as applications, operating systems, databases, and supporting IT infrastructure. The general objective for ITGC is to ensure the integrity of the data and processes that systems support.

To provide additional insight into these sensitive recommendations, we categorized the recommendations from sensitive IT engagements into the following ITGC areas:

ITGC	Description of control
<b>Data Backup and Recovery</b>	Controls provide reasonable assurance that data and systems are backed up successfully, completely, stored offsite, and validated periodically.
<b>Environmental</b>	Controls provide reasonable assurance that systems equipment and data is adequately protected from environmental factors.
<b>Information Security</b>	Controls provide reasonable assurance that policies and procedures are in place to ensure effective communication of information security practices.
<b>Logical Access</b>	Controls provide reasonable assurance that logical access to applications and data is limited to authorized individuals.
<b>Physical Security</b>	Controls provide reasonable assurance that physical access to systems equipment and data is restricted to authorized personnel.
<b>System Development &amp; Change Management</b>	Controls provide reasonable assurance that changes to or development of applications is authorized, tested, and approved. Controls also, provide reasonable assurance that segregation of duties exist.
<b>System Monitoring &amp; Maintenance</b>	Controls provide reasonable assurance that systems are monitored for security issues, and that patches and antivirus definition file updates are applied in a timely manner.

**Table 2: Recommendations Status – By IT General Control Areas**

	Total Recos	Implemented During Prior Periods	Implemented Nov 2023 – Feb 2024	In Progress Mar 2024
Data Back Up & Recovery	2	1	1	—
Environmental	—	—	—	—
Information Security	18	8	2	8
Logical Access	49	45	2	2
Physical Security	3	—	2	1
System Development & Change Management	2	2	—	—
System Monitoring & Maintenance	19	14	2	3
<b>Total by Implementation Status</b>	<b>93</b>	<b>70</b>	<b>9</b>	<b>14</b>

Recommendation Follow-Up for Sensitive Information Technology Areas

March 6, 2024

Page 5 of 5

Internal Audit will continue to update the Audit Committee on the status of recommendations at each Committee meeting.

Staff will be available to address questions at the March 18, 2024, Audit Committee meeting, but please remember that due to the sensitive nature of these IT recommendations we cannot provide additional details.

Noted and Reviewed:



---

Richard P. Bendall  
Chief Audit Executive

GT

**FOR INFORMATION ONLY**

March 5, 2024

TO: 2024 Audit Committee  
 Nancy M. Durazo, BOR Trustee  
 Vivian H. Gray, BOR Trustee  
 Wayne Moore, BOR Trustee  
 Jason E. Green, BOI Trustee  
 Debbie Martin, BOI Trustee  
 Herman B. Santos, BOI Trustee  
 Keith Knox, Ex-Officio

Audit Committee Consultant  
 Larry Jensen

FROM: Leisha E. Collins   
 Principal Internal Auditor

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Ethics Hotline Status Report**

**BACKGROUND**

The purpose of this memorandum is to provide the Committee with information on ethics cases handled by LACERA. Since November 2019, LACERA has contracted with NAVEX Global's EthicsPoint Hotline for ethics reporting and case management needs.

There are no open cases and five cases have been closed since the December 2023 Committee meeting as reported in the table below:

Case #	Month Received	Issue	Case Assignment	Status	Month Closed	Control Deficiencies Identified from Case
14	June 2023	Conflict of Interest	Legal/External Investigator	Investigation complete	Feb 2024	None
15	June 2023	Inappropriate Supervisor Directive	Legal/External Investigator	Investigation complete	Feb 2024	None
16	June 2023	Policy Violation	Legal/External Investigator	Investigation complete	Feb 2024	None
18	September 2023	Confidentiality and Misappropriation	Legal/External Investigator	Investigation complete	Feb 2024	None
19	September 2023	Inappropriate Supervisor Directive	Legal/External Investigator	Investigation complete	Feb 2024	None

Ethics Hotline Status Report

March 5, 2024

Page 2 of 2

Staff will continue to provide updates to the Committee on future reports. For the Committee's information, Internal Audit is not currently investigating, nor has it received any new reports of wrongdoing and/or become aware of any matters of wrongdoing outside of the Ethics Hotline. Furthermore, we have not identified any matters of fraud in any of our recent or current audit and consulting work.

Noted and Reviewed:



---

Richard P. Bendall  
Chief Audit Executive

RPB:lec

**FOR INFORMATION ONLY**

March 5, 2024

TO: 2024 Audit Committee  
Nancy M. Durazo, BOR Trustee  
Vivian H. Gray, BOR Trustee  
Wayne Moore, BOR Trustee  
Jason E. Green, BOI Trustee  
Debbie Martin, BOI Trustee  
Herman B. Santos, BOI Trustee  
Keith Knox, Ex-Officio

Audit Committee Consultant  
Larry Jensen

FROM: Richard P. Bendall   
Chief Audit Executive

FOR: March 18, 2024 Audit Committee Meeting

SUBJECT: **Internal Audit Staffing Activity Report**

At the request of the Audit Committee, at each meeting, we provide this Staffing Activity Report, to keep the Committee abreast of audit resources impacting current work and future planning.

Internal Audit has 11 budgeted positions, one Chief Internal Auditor, two Principal Internal Auditors, six Senior Internal Auditors, one Internal Auditor and one Senior Administrative Assistant.

We currently have the following vacancies:

- One Senior Internal Auditor position which was vacated in July 2020 when the employee was transferred to the Systems Division.
- One Senior Internal Auditor position which was vacated in July 2023 when the employee was transferred to the Investments Office.
- One Internal Auditor position which was vacated in October 2021 when the employee was promoted to a Senior Internal Auditor.

Additionally, of the four current Seniors, one is on leave until the end of June 2024.

We are pleased to inform the Committee that we are currently working with HR to begin the hiring process for the two vacant Senior positions and the vacant Internal Auditor position. In the interim, we have adjusted our Audit Plan for the year to address the current staff shortages.

I look forward to addressing any questions you may have at your March meeting.

RPB:rb



---

**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**