



Alameda County Employees' Retirement Association
BOARD OF RETIREMENT

AUDIT COMMITTEE/BOARD MEETING
NOTICE and AGENDA

ACERA MISSION:

To provide ACERA members and employers with flexible, cost-effective, participant-oriented benefits through prudent investment management and superior member services.

Thursday, February 20, 2025
12:30 p.m.

LOCATION AND TELECONFERENCE	COMMITTEE MEMBERS	
<p>ACERA C.G. "BUD" QUIST BOARD ROOM 475 14TH STREET, 10TH FLOOR OAKLAND, CALIFORNIA 94612-1900 MAIN LINE: 510.628.3000 FAX: 510.268.9574</p> <p>The public can observe the meeting and offer public comment by using the below Webinar ID and Passcode after clicking on the below link or calling the below call-in number.</p> <p>Link: https://zoom.us/join Call-In: 1 (669) 900-6833 US Webinar ID: 879 6337 8479 Passcode: 699406 For help joining a Zoom meeting, see: https://support.zoom.us/hc/en-us/articles/201362193</p>	HENRY LEVY, CHAIR	TREASURER
	TARRELL GAMBLE, VICE-CHAIR	APPOINTED
	ROSS CLIPPINGER	ELECTED SAFETY
	STEVEN WILKINSON	APPOINTED
	GEORGE WOOD	ELECTED GENERAL

The Alternate Retired Member votes in the absence of the Elected Retired Member, or, if the Elected Retired Member is present, then votes if both Elected General Members, or the Safety Member and an Elected General Member, are absent.

The Alternate Safety Member votes in the absence of the Elected Safety Member, either of the two Elected General Members, or both the Retired and Alternate Retired Members.

This is a meeting of the Audit Committee if a quorum of the Audit Committee attends, and it is a meeting of the Board if a quorum of the Board attends. This is a joint meeting of the Audit Committee and the Board if a quorum of each attends.

Note regarding accommodations: If you require a reasonable modification or accommodation for a disability, please contact ACERA between 9:00 a.m. and 5:00 p.m. at least 72 hours before the meeting at accommodation@acera.org or at 510-628-3000.

Public comments are limited to four (4) minutes per person in total. The order of items on the agenda is subject to change without notice. Board and Committee agendas and minutes and all documents distributed to the Board or a Committee in connection with a public meeting (unless exempt from disclosure) are posted online at www.acera.org and also may be inspected at 475 14th Street, 10th Floor, Oakland, CA 94612-1900.

AUDIT COMMITTEE/BOARD MEETING

NOTICE and AGENDA, Page 2 of 2 - Thursday, February 20, 2025

Call to Order

12:30 p.m.

Roll Call

Public Input (Time Limit: 4 minutes per speaker)

Action Items: Matters for Discussion and Possible Motion by the Committee

- 1. Presentation, discussion, and possible motion to approve the external audit scope of work and timeline of services for the Financial Statements ended December 31, 2024, performed by Williams, Adley & Company-CA, LLP**

- Robert Griffin, Partner
- Kenneth Yu, Sr. Manager
Williams, Adley & Company-CA, LLP
- Erica Haywood

Recommendation:

The Audit Committee recommends to the Board of Retirement that the Board approve the external audit scope of work and timeline of services for the Financial Statements ended December 31, 2024, to be performed by Williams, Adley & Company-CA, LLP.

Information Items: These items are not presented for Committee action but consist of status updates and cyclical reports.

External Audit

- 1. 2025 Audit Committee Work Plan (Proposed)** - Lisa Johnson

Internal Audit

- 1. Review of Annual Risk Assessment** - Harsh Jadhav
- 2. Presentation of the 2025 Internal Audit Plan (Proposed)** - Harsh Jadhav
- 3. Audit Results - Member Direct Deposit (Fraud) Audit** - Caxton Fung
- 4. Cybersecurity Update** - Vijay Jagar

Trustee Remarks

Future Discussion Items

Establishment of Next Meeting Date

April 17, 2025



MEMORANDUM TO THE AUDIT COMMITTEE

DATE: February 20, 2025

TO: Members of the Audit Committee

FROM: Erica Haywood, Fiscal Services Officer *EH*

SUBJECT: **Williams, Adley & Co. LLP., 2024 Financial Statement External Audit**

The Fiscal Services Department has reviewed the 2024 external audit scope of work and timeline of services to be performed by Williams, Adley, & Co. LLP, ACERA is prepared to commence with its annual financial statement audit for year ended December 31, 2024. The allotted time frame of the audit field work is approximately 60 days, ending approximately the third week in April 2025.

Throughout the audit period, bi-weekly status meetings with the Fiscal Services Department will be conducted. Likewise, status meetings with Senior Leaders will also be scheduled on an as needed basis. The Fiscal Services Officer will oversee the audit process and is responsible for ensuring the completeness and accuracy of all financial information provided to Williams, Adley, & Co. LLP.

Recommendation

Staff recommends that the Audit Committee recommend to the Board of Retirement that the Board approve the 2024 Financial Statement External Audit Scope of Work and Timeline of Services to be performed by Williams, Adley & Co. LLP.



ALAMEDA COUNTY EMPLOYEES' RETIREMENT ASSOCIATION

Audit and Communications Plan for the Year Ended
December 31, 2024



Confidence Earned

Agenda

- ▶ Engagement Team
- ▶ Auditor Responsibilities
- ▶ Management Responsibilities
- ▶ Audit Committee Responsibilities
- ▶ Our Risk-Based Audit Approach
- ▶ Areas of Significant Focus
- ▶ Areas of Audit Emphasis
- ▶ Timeline
- ▶ Accounting and Auditing Standards Changes

Engagement Team

- ▶ Robert Griffin, CPA, Engagement Partner
 - ▶ Has overall responsibility for the engagement, including service levels and adherence to timelines. Responsible for the engagement, including the content of reports and compliance with firm and professional standards.
- ▶ Kenneth Yu, CPA, Project Manager
 - ▶ Primarily responsible for the achievement of engagement objectives and quality control of the audit procedures performed and the reports issued. He will serve as the primary liaison between ACERA staff and WACO team members and have responsibility for achieving the audit objectives.

Auditor Responsibilities

- ▶ Our responsibility under U.S. Generally Accepted Auditing Standards and *Government Auditing Standards* is to express opinions about whether the financial statements prepared by management with your oversight are fairly presented, in all material respects, in conformity with U.S. GAAP. Provide an in-relation to opinion on the other supplementary information.
- ▶ Issue report on internal controls and compliance (no opinion) based on results of tests of compliance with certain provisions of laws, regulations, contracts and grants
- ▶ Perform an audit of the GASB 68 & GASB 75 schedules in accordance with GAAS.
- ▶ Express opinions on whether the GASB 68 & GASB 75 schedules are fairly presented in conformity with U.S. GAAP.
- ▶ Communicate significant matters related to the audits.

Management Responsibilities

- ▶ Prepare and present financial statements and supplementary information in conformity with U.S. GAAP.
- ▶ Establish and maintain effective internal controls.
- ▶ Implement systems designed to achieve compliance with applicable laws, regulations, and contracts.
- ▶ Select and apply appropriate accounting principles.
- ▶ Comply with applicable laws and regulations and the provisions of contracts.
- ▶ Design and implement programs and controls to prevent and detect fraud, and inform us about all known or suspected fraud.
- ▶ Provide written representations.

Audit Committee Responsibilities

- ▶ Meet periodically with the auditors to discuss various topics, including risks, concerns about internal controls, significant communications with regulators, and audit progress.
- ▶ Resolve conflicts between auditors and management, if necessary.
- ▶ Review auditor's findings and recommendations and evaluate management's response.

Our Risk-Based Audit Approach

- ▶ Audit planning is a continuous process.
- ▶ Identification of current external and internal risks.
- ▶ Internal control testing and evaluation - Narratives, walkthroughs, and rotational testing.
- ▶ Materiality - Emphasis on areas with greater possibility of material errors.
- ▶ Reporting objectives - Fairness, clarity and accuracy.
- ▶ Our risk assessment is the basis for our audit programs. Throughout the audit, we continuously monitor and update our risk assessment and approach.

Areas of Significant Focus

Additions (Revenue)	Benefits (Expense)
<p><u>Risks</u></p> <ul style="list-style-type: none">▪ Contributions are misstated.▪ Investment income, including appreciation, is misstated.	<p><u>Risks</u></p> <ul style="list-style-type: none">▪ Conversion to Pension Gold v3 during the year.▪ Benefit expense could be misstated.
<p><u>Audit Response</u></p> <ul style="list-style-type: none">▪ Confirm contributions and related receivables with employers.▪ Confirm investment income and perform analytical procedures.	<p><u>Audit Response</u></p> <ul style="list-style-type: none">▪ Review completion reports from outside consultants.▪ Review Problem Incident Reports (PIR) submitted by ACERA after the transition.▪ Control testing over new retirees and their benefit payments.

Areas of Significant Focus (continued)

Management Override of Controls	Investments
<p><u>Risks</u></p> <ul style="list-style-type: none">▪ Financial statements could be materially misstated.▪ Misappropriation of assets.	<p><u>Risks</u></p> <ul style="list-style-type: none">▪ Misstatement of account balances.▪ Appropriate valuation of investments, particularly alternative investments.▪ Transactions reported in incorrect period.▪ Assets not held in ACERA's name.
<p><u>Audit Response</u></p> <ul style="list-style-type: none">▪ Evaluate and update our understanding of controls over the financial reporting process.▪ Select a sample of transactions and test to determine if controls are operating effectively.	<p><u>Audit Response</u></p> <ul style="list-style-type: none">▪ Independent confirmation and reconciliation testing.▪ Review of third party valuations and market quotes.

Other Areas of Audit Emphasis

- ▶ In addition to the significant areas identified previously, we have identified areas below as areas of focus during the audit due to materiality of the balance and/or complexity or judgment involved in the accounting.
 - ▶ Participant data and actuarial information
 - ▶ Reserves
 - ▶ Cash activity
 - ▶ Accounting and reporting for actuarial assumptions and calculations used as a basis to measure the pension liability.
 - ▶ Financial reporting

Timeline

- ▶ Planning and client assistance - January / February 2025
- ▶ Fieldwork - Mid February - April 2025
- ▶ Presentation of Audit Results to Audit Committee - May 2025
- ▶ Reporting Deadlines
 - ▶ State Controller's Report - June 30, 2025
 - ▶ ACFR to GFOA - June 30, 2025
- ▶ GASB 68 & 75 reports - June 2025

Accounting Standards Changes

- ▶ Statement No. 100 - *Accounting Changes and Error Corrections*
 - ▶ The primary objective of this Statement is to enhance the accounting and financial reporting requirements for accounting changes and error corrections to provide more understandable, reliable, relevant, consistent, and comparable information for making decisions or assessing accountability.

- ▶ Statement No. 101 - *Compensated Absences*
 - ▶ The objective of this Statement is to better meet the information needs of financial statement users by updating the recognition and measurement guidance for compensated absences. That objective is achieved by aligning the recognition and measurement guidance under a unified model and by amending certain previously required disclosures.

Auditing Standards Changes

- ▶ Statement on Auditing Standards (SAS) 143 - *Auditing Accounting Estimates and Related Disclosures*
 - ▶ This standard emphasizes the importance of understanding management's process for developing accounting estimates and outlines specific items required to be considered during the risk assessment phase of the audit.
- ▶ SAS 145 - *Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement*
 - ▶ This standard enhances requirements and guidance related to the auditor's risk assessments, particularly related to understanding ACERA's system of internal control and required auditing to obtain the necessary understanding of the internal control system. This also includes increased focus related to IT risk.



MEMORANDUM TO THE AUDIT COMMITTEE

DATE: February 20, 2025

TO: Members of the Audit Committee

FROM: Lisa Johnson, Assistant Chief Executive Officer
Harsh Jadhav, Chief of Internal Audit

SUBJECT: **Proposed 2025 Audit Committee Work Plan**

A handwritten signature in blue ink, appearing to read 'L. Johnson'.

The proposed 2025 Audit Committee Work Plan is attached for your consideration and review. The main action and topical discussion items for 2025 are listed below for quick reference:

- February 20, 2025
 - Williams, Adley & Co. LLP. will present the external audit scope of work and timeline of services for the financial statements ended December 31, 2024.
- April 17, 2025
 - Presentation and discussion of the Government Accounting Standards Board (GASB) Statement No. 67 and No. 74 Valuations and addendums as of December 31, 2024 (Segal).
- May 22, 2025
 - External auditor's report and presentation of December 31, 2024, audited financial statements.
 - Recommend adoption of the GASB Statement No. 67 and No. 74 Valuations and addendums as of December 31, 2024.
- June 18, 2025:
 - Adoption of the audited Schedules of Employer Allocations and Schedules of Pension and OPEB Amounts by Employer; and
 - Presentation of the GASB Statement No. 68 and No. 75 Valuations and Employer Schedules as of December 31, 2024.
- October 16, 2025:
 - Progress Report on the Internal Audit Plan

Throughout the year, ACERA's Chief of Internal Audit will review the progress of the internal audit plan, present new internal audit initiatives, and review completed audits. As the need arises, agenda items may be changed or added to the work plan during the year.



2025 Audit Committee Work Plan (Proposed)

	Action Items	Information Items
<p>Feb 20 – 12:30 PM (3rd Thurs, same day as Board Meeting)</p>	<p>External Audit</p> <ul style="list-style-type: none"> • Presentation, discussion, and possible motion to approve the external audit scope of work and timeline of services for the Financial Statements ended December 31, 2024, performed by the external audit firm <p>Internal Audit</p> <ul style="list-style-type: none"> • None 	<p><i>External Audit</i></p> <ul style="list-style-type: none"> • 2025 Audit Committee Work Plan (Proposed) <p><i>Internal Audit</i></p> <ul style="list-style-type: none"> • Review of Annual Risk Assessment • Presentation of the 2025 Internal Audit Plan • Cybersecurity Update
<p>Apr 17 – 12:30 PM (3rd Thurs, same day as Board Meeting)</p>	<p><i>External Audit</i></p> <ul style="list-style-type: none"> • None <p><i>Internal Audit</i></p> <ul style="list-style-type: none"> • None 	<p><i>External Audit</i></p> <ul style="list-style-type: none"> • Presentation and discussion of the GASB Statement No. 67 Valuation and addendum as of December 31, 2024 (Segal) • Presentation and discussion of the GASB Statement No. 74 Valuation and addendum as of December 31, 2024 (Segal) <p><i>Internal Audit</i></p> <ul style="list-style-type: none"> • Progress report on the Internal Audit Plan • Review complete audits and projects

Note: This work plan is subject to change without prior notice. Periodic rearrangements of agenda items will be made to the work plan to provide a reasonable length of time for each meeting.



2025 Audit Committee Work Plan (Proposed)

Action Items

Information Items

<p>May 22 – 12:30 PM (Moved due to SACRS, same day as Board Meeting)</p>	<p><i>External Audit</i></p> <ul style="list-style-type: none">• Discussion and possible motion to recommend that the Board of Retirement accept and file the December 31, 2024 Audited Financial Statements and Independent Auditor’s Report• Discussion and possible motion to recommend that the Board of Retirement adopt of the Government Accounting Standards Board (GASB) Statement No. 67 Actuarial Valuation and addendum as of December 31, 2024• Discussion and possible motion to recommend that the Board of Retirement adopt the Government Accounting Standards Board (GASB) Statement No. 74 Actuarial Valuation and addendum as of December 31, 2024 <p><i>Internal Audit</i></p> <ul style="list-style-type: none">• None	<p><i>External Audit</i></p> <p><i>Internal Audit</i></p> <ul style="list-style-type: none">• Progress Report on the Internal Audit Plan• Review completed audits and projects
-----------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



2025 Audit Committee Work Plan (Proposed)

	Action Items	Information Items
Jun 18 – 12:30 PM (Moved due to holiday, same day as Board Meeting)	<i>External Audit</i> <ul style="list-style-type: none">Review and possible motion to adopt the audited Schedule of Employer Allocations (Pension and OPEB) and the audited Schedule of Pension and OPEB Amounts by Employer based on addenda to the Governmental Accounting Standards Board (GASB) Statement No. 67 and Statement No. 74, valuations as of December 31, 2024 <i>Internal Audit</i> <ul style="list-style-type: none">None	<i>External Audit</i> <ul style="list-style-type: none">Presentation and discussion of GASB Statement No. 68 and GASB Statement No. 75 Valuations and Employer Schedules as of December 31, 2024 <i>Internal Audit</i> <ul style="list-style-type: none">Progress Report on the Internal Audit PlanReview completed audits and projects
Oct 16 - 12:30 PM (3 rd Thurs, same day as Board Meeting)	<i>External Audit</i> <ul style="list-style-type: none">None <i>Internal Audit</i> <ul style="list-style-type: none">None	<i>External Audit</i> <ul style="list-style-type: none">None <i>Internal Audit</i> <ul style="list-style-type: none">Progress Report on the Internal Audit PlanReview completed audits and projects

Note: This work plan is subject to change without prior notice. Periodic rearrangements of agenda items will be made to the work plan to provide a reasonable length of time for each meeting.



MEMORANDUM TO THE AUDIT COMMITTEE

DATE: February 20, 2025

TO: Members of the Audit Committee

FROM: Harsh Jadhav, Chief of Internal Audit

SUBJECT: The Proposed 2025 Internal Audit Program

Overview of the February 2025 Meeting Agenda

The February 2025 Audit Committee meeting will include the presentation of the proposed 2025 Internal Audit Program, a discussion of the risk assessment process, the presentation of the Member Direct Deposit Audit results, and a cybersecurity update. These agenda items provide a snapshot of the current and emerging risks, an audit program to focus on the highest priority risks based on available resources, and a plan to continue educating trustees and staff on changes in the threat landscape and risk mitigation strategies to safeguard organizational assets.

Risk Assessment Process and Outcomes

The annual risk assessment has been completed. Risks identified by management were reassessed to evaluate the impact of changes in business processes, legislation, pension practices, and organizational structure on internal controls. During the meeting, we will summarize the key departmental risks identified by staff and their potential implications for internal controls and fraud risks.

Based on the risk assessment results, the Internal Audit Department has outlined the following initiatives for 2025:

- Conduct three internal audits.
- Perform one employer audit
- Undertake three special projects.
- Deliver fraud awareness training to staff.

These initiatives reflect our commitment to addressing significant risks and enhancing the organization's control environment.

Member Direct Deposit Audit Results

The Member Direct Deposit Audit was a limited-scope audit to review the internal controls protecting member accounts and banking information. Staff will review the testing methodology, positive results, and recommendations from the audit.

Cybersecurity and Data Security Education

The Internal Audit Department continues to collaborate with PRISM to advance cybersecurity and data security awareness. PRISM's regular self-assessments encompass reviews of incident response procedures, security management processes, IT infrastructure, and cybersecurity training. These efforts identify gaps, potential vulnerabilities, and threats, ensuring robust defenses for protecting sensitive information.

Moreover, these initiatives are critical to supporting the upgraded pension system by maintaining a resilient IT infrastructure. As part of this discussion, Vijay Jagar will provide a cybersecurity update focusing on recent trends in phishing and ransomware threats.

Fraud Awareness and Training

Promoting fraud awareness remains a priority for the Internal Audit Department. This year, we will expand our fraud training efforts to include organization-wide sessions that emphasize protecting member information and fund assets. Additionally, Internal Audit team members will continue to serve as resources for enhancing internal controls across the organization.

We look forward to discussing these initiatives and updates in greater detail during the February meeting. Your input and guidance will be invaluable as we advance these objectives.

2025 Proposed Audit Schedule

Internal Audit Plan (2025)	Service Line	Assigned	Status	Q1	Q2	Q3	Q4
Member Direct Deposit(Fraud) Audit	Internal Audit	Caxton	Completed	Green			
System-Wide Benefit Overpayment - Final Average Salary Audit	Internal Audit	Caxton	Not Started	Brown	Brown	Brown	
Workforce Resilience (Critical Functions) Audit	Internal Audit	Marlon, Dana, Lyndon, Harsh	Continuous	Yellow	Yellow	Yellow	Yellow
401(1) 17 Cap Limitation Audit	Employer Audit	Caxton	Not Started			Grey	Grey
Data Cleanup Review	Special Project	Lyndon	Not Started	Red	Red		
Third-Party Service Provider Review	Special Project	Harsh	Not Started				Purple
Investment Manager Fee Review	Special Project	Harsh	Not Started			Blue	Blue
Cybersecurity and Data Security Education	Administration	Vijay, Harsh	Continuous	Orange	Orange	Orange	Orange
2025 Annual Risk Assessment	Administration	Harsh	Completed	Green			
2026 Annual Risk Assessment	Administration	Harsh	Not Started				Grey
Fraud Hotline Management	Administration	Lyndon, Harsh	Continuous	Pink	Pink	Pink	Pink
Fraud Training	Administration	Lyndon, Caxton	Not Started			Grey	

2025 Proposed Audit Program

Internal Audits

Member Direct Deposit (Fraud) Audit

This audit aims to enhance internal controls by assessing potential fraud risks related to unauthorized attempts to change a member’s bank account information through the member portal or standard change request processes. A joint member authentication survey conducted by ACERA and CALAPRS revealed growing concerns among retirement systems regarding members using virtual-only banks. This audit will address these concerns by evaluating existing authentication protocols and identifying areas for improvement to mitigate fraud risks.

System-Wide Benefit Overpayment Audit – Final Average Salary Calculation Audit

The purpose of this audit is to ensure the accuracy and consistency of internal controls designed to prevent benefit overpayments for active, deferred, and retired members. Our approach involves conducting targeted, small-sample audits to identify potential vulnerabilities in the calculation of Final Average Salary (FAS) and monthly retirement benefits. Key areas of focus include payroll data accuracy, member years of service, reciprocity arrangements (if applicable), vacation sell, court orders, and unusual

scenarios. This methodology allows us to detect systemic issues efficiently and propose actionable recommendations for remediation.

Workforce Resilience Audit

This review evaluates ACERA's preparedness to sustain critical processes during periods of disruption. Specifically, it assesses whether staff are adequately trained, backup personnel are identified and equipped to perform critical tasks, and essential processes are documented and updated regularly. Given the ongoing challenges posed by cybersecurity and other adverse events, this audit supports business continuity by ensuring that ACERA maintains operational resilience.

Employer Audits

401(a) 17 Cap Limitation Audit

The objective of this audit is to verify compliance with the IRS 401(a) 17 limit under Title 26 of the United States Code and PEPRA new tier wage limits. This involves reviewing the capping of Final Average Salary calculations by ACERA and participating employers. Sample testing of select employers will assess the effectiveness of their internal controls and ACERA's oversight in ensuring timely halting of contributions when limits are reached.

Special Projects

Data Cleanup Review

This project focuses on reviewing benefit databases and applications for accuracy and completeness. Online files and folders will be examined to ensure required documentation for administering retirement benefits, such as death certificates, is properly stored, accessible, and up to date.

Third-Party Service Provider Review

This review assesses whether critical third-party service providers managing ACERA's confidential and sensitive information have adequate insurance coverage, robust internal controls to prevent data breaches, effective adverse event management processes, and sufficient incident response procedures.

Investment Manager Fee Review

The goal of this review is to ensure the accuracy and appropriateness of fees paid to investment managers. It includes a thorough evaluation of fee agreements, such as management and performance fee structures, to confirm compliance with contractual terms. Transaction records, account statements, and invoices will be analyzed to verify calculations, adherence to regulatory standards, and alignment with industry practices. This review will identify any discrepancies, overpayments, or inefficiencies and recommend measures to strengthen financial controls.

Cybersecurity and Data Security Education

This special project, in collaboration with the PRISM Department, evaluates the adequacy of employee training and processes for incident response, business recovery, and threat analysis. It aims to ensure that sensitive organizational and member data are protected against emerging cybersecurity threats.

Summary

We remain committed to achieving the 2025 Audit Program objectives. I would like to recognize the Internal Audit Staff for their dedication and exceptional work in partnering with management, supporting the Board of Retirement, and safeguarding our members. Their efforts continue to uphold ACERA's mission of integrity and accountability.

Internal Audit Department 2025 Internal Audit Plan

February 20, 2025

Agenda



Review the Risk
Assessment Process




Proposed Internal
Audit Plan



Member Direct
Deposit Audit Results

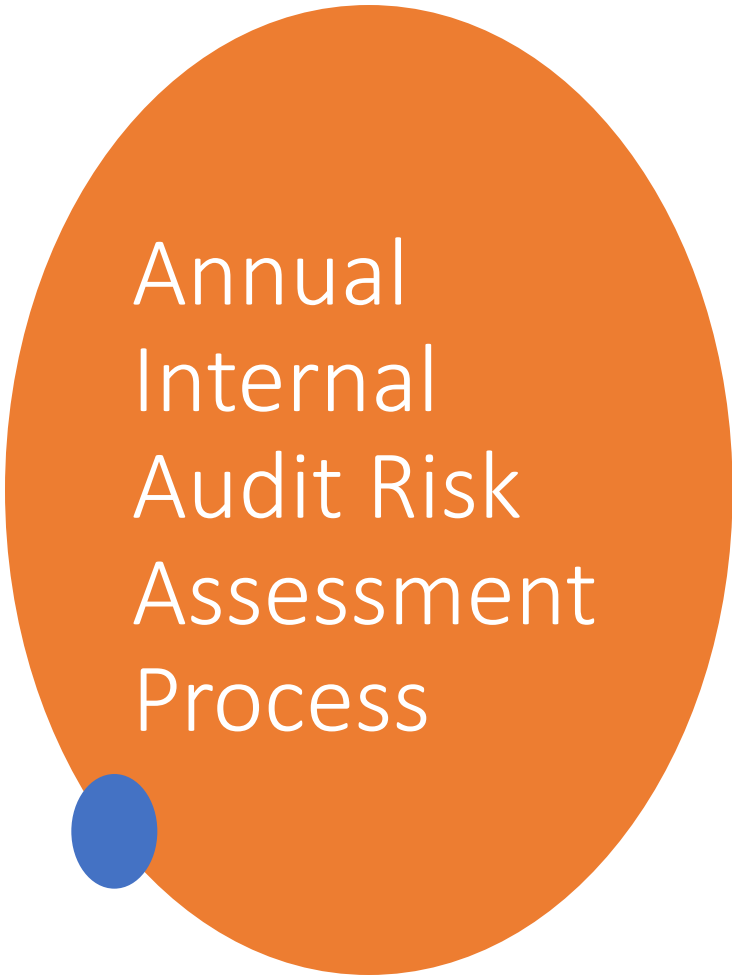


Cybersecurity
Update



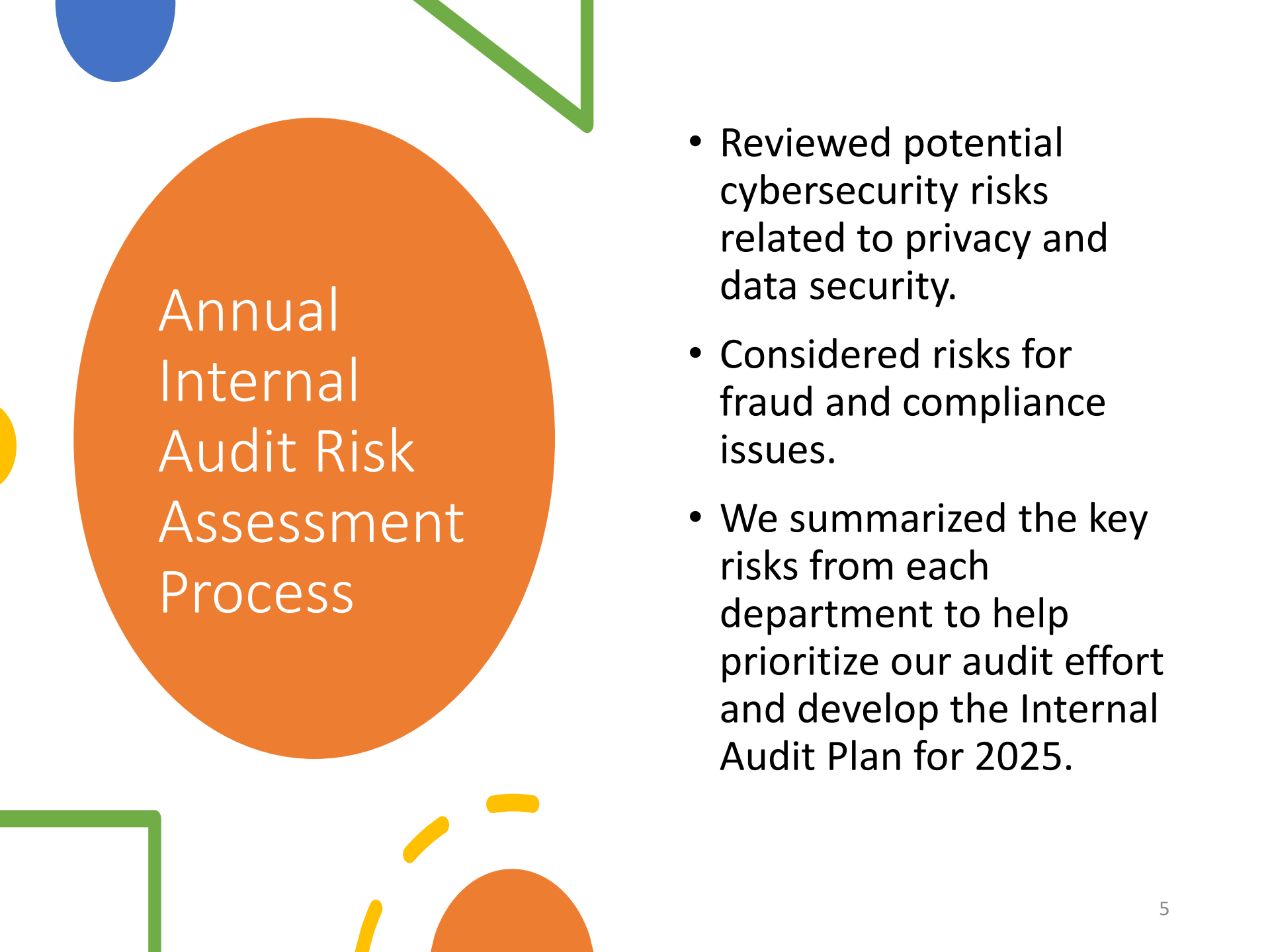
Annual Internal Audit Risk Assessment Process

- Reviewed the strategic objectives of each department and current and potential risks the departments were concerned about. The department-level risks covered benefits, fiscal operations, investments, legal, IT, actuarial and human resources.



Annual Internal Audit Risk Assessment Process

- Assessed potential control weaknesses, new business processes introduced in the current year, staffing changes, and new legislative mandates which may impact the current business.



Annual Internal Audit Risk Assessment Process

- Reviewed potential cybersecurity risks related to privacy and data security.
- Considered risks for fraud and compliance issues.
- We summarized the key risks from each department to help prioritize our audit effort and develop the Internal Audit Plan for 2025.

Identified Risks

- Investment Bank Reporting
- Retaining Key Personnel and Retirements
- Third-Party Security Assessments
- Privacy of Human Resource Data

Operations

- 401(a) (17) Limitations
- Disability Retirement
- Final Average Salary Calc.
- Employer Pay Code Set Up and Usage
- Benefit Recipient Certification

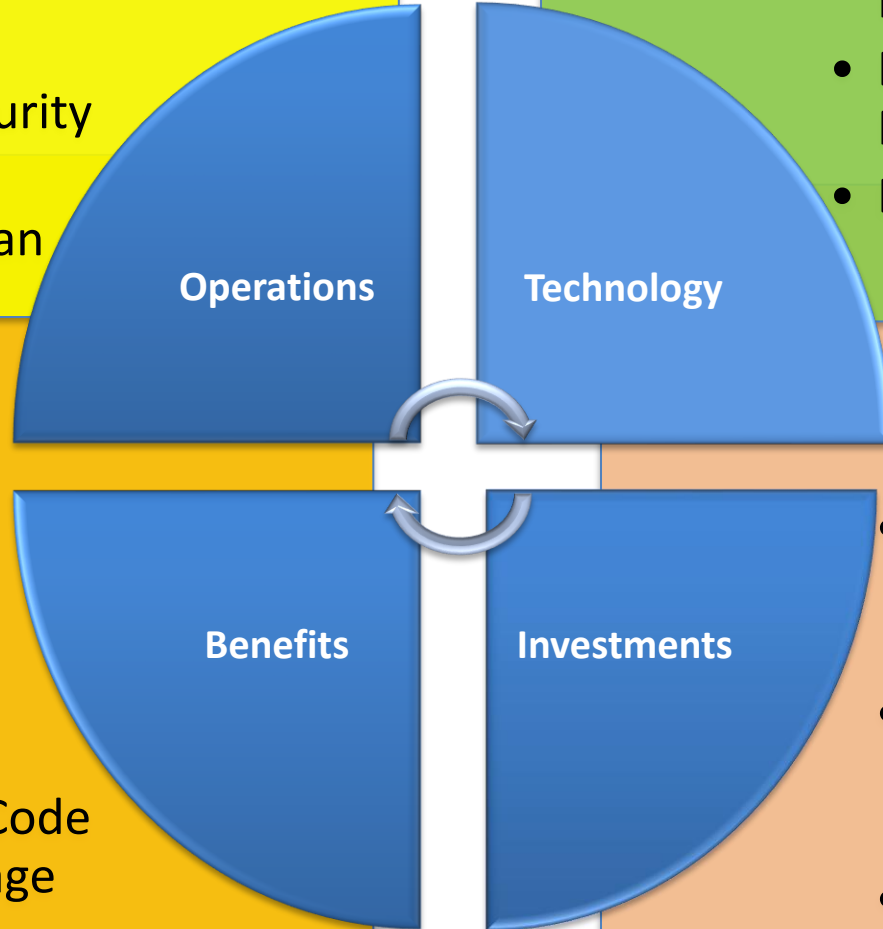
Benefits

- ONBASE Upgrade
- Cybersecurity
- Business Continuity Planning
- Document Management
- Data Cleanup

Technology

- Implementation of the Board Approved Asset Allocation
- Integrating New General Investment Consultant
- Investment Manager Fee Review

Investments



Proposed 2025 Internal Audit Plan

Internal Audit Plan (2025)	Service Line	Assigned	Status	Q1	Q2	Q3	Q4
Member Direct Deposit(Fraud) Audit	Internal Audit	Caxton	Completed				
System-Wide Benefit Overpayment - Final Average Salary Audit	Internal Audit	Caxton	Not Started				
Workforce Resilience (Critical Functions) Audit	Internal Audit	Marlon, Dana, Lyndon, Harsh	Continuous				
401(1) 17 Cap Limitation Audit	Employer Audit	Caxton	Not Started				
Data Cleanup Review	Special Project	Lyndon	Not Started				
Third-Party Service Provider Review	Special Project	Harsh	Not Started				
Investment Manager Fee Review	Special Project	Harsh	Not Started				
Cybersecurity and Data Security Education	Administration	Vijay, Harsh	Continuous				
2025 Annual Risk Assessment	Administration	Harsh	Completed				
2026 Annual Risk Assessment	Administration	Harsh	Not Started				
Fraud Hotline Management	Administration	Lyndon, Harsh	Continuous				
Fraud Training	Administration	Lyndon, Caxton	Not Started				

MEMBER DIRECT DEPOSIT AUDIT 2024



Auditing for Fraud:

Background:

In 2023, the Internal Audit Department launched a member authentication process survey to assess the effectiveness of security measures across all 1937 Act retirement systems.

A total of 19 retirement systems responded to the 22-question survey.

The survey results revealed a new risk: some retirement systems reported incidents in which external fraudsters attempted to change the direct deposit bank account information for members receiving pension benefits. This finding highlighted a critical vulnerability. To better assess and mitigate the risks associated with direct deposits, the Internal Audit Department launched a comprehensive audit—our first audit specifically focused on member fraud prevention.

Audit Objective

The objective of this audit is to identify any suspicious or fraudulent activities related to recent direct deposit bank account change requests.

Given the evolving nature of fraud schemes and the ongoing volume of member change requests, we have implemented audit technology to allow our team to run a recurring audit on a periodic basis. This audit will serve as a valuable reference for future audits, enhancing efficiency and reducing the time required to conduct similar assessments moving forward.

Summary of Audit Scope & Strategy

- Internal Audit Department conducted a limited-scope audit to the Member Direct Deposit
- The primary focus of this audit was to review recent member account requests involving changes to bank accounts with fintech banks and virtual-only banks, such as Green Dot Bank, Capital One, Discover, Credit Karma, etc.
- Please note that this audit's scope did not include the network and system security for the Pension Gold (PG) system and the Member Direct (MD) user portal.
- By using data analytics software, we matched approximately 22,000 routing number records from two monthly ACH files (PG system version 2) against the list of bank routing numbers.
- We authenticated the signature on the most recent change request form and compared it to signatures on earlier documents.
- Benefits Department kindly provided a walkthrough of the direct deposit account request process in PG version 3 and the MD portal.

- We reviewed the routing numbers from the April and September 2024 ACH files, each containing approximately 11,000 pension benefit payment records & routing numbers.
- Additionally, we proactively searched for known routing numbers from fintech and virtual-only banks that were not yet used by our members and added them to our list. Some of the banks included in this search were:
 - Chime Bank
 - Current Bank
 - Cash App
 - Stride Bank
 - Dave Bank
 - Wise App
 - Credit Karma
 - Brex Bank
 - Green Dot Bank
- We compiled a comprehensive list of over 600 routing numbers specific to ACERA membership and matched the routing numbers from the bank institution list and the ACH files using data analytics software. We then selected samples primarily from the highest risk of direct deposit account requests that involved switches to virtual-only banks for further review.

CONTROL 1 – VERIFICATION OF THE DIRECT DEPOSIT ACCOUNT CHANGE REQUEST

We examined selected monthly ACH files to identify potential suspicious or fraudulent activities.

Test Note:

- we compared the signature on the form with signatures from earlier documents to validate the authenticity of the bank account change request.
- Based on our review of the samples, we found no evidence of fraudulent activities in the 2024 direct deposit account change requests.
- In some cases, we noted that the Retirement Technician (RT) had left a note indicating they contacted the member directly to verify the change request.
- Given that other retirement systems have reported potential fraudulent activity associated with Green Dot Bank, we reviewed all three members' direct deposit change requests, regardless of when the requests were submitted. In each case, the member had either provided an identification card or had been contacted by the RT to confirm the request.

Recommendations

:

1. As fraud schemes are constantly evolving, and new banks and routing numbers are frequently added, we recommend conducting a fraud audit every three to six months, depending on the workload of the Internal Audit Department. This practice can help identify and address direct deposit fraud more promptly, should it occur.
2. Members who change their direct deposit bank accounts, particularly those using virtual-only banks (e.g., Chime, SoFi, etc.), represent a higher risk, as recovering misappropriated funds is more difficult. To mitigate this risk, we recommend that members submit a copy of their driver's license, passport, or another government-issued ID along with their change request.

CONTROL 2 – DIRECT DEPOSIT ACCOUNT CHANGE REQUEST THROUGH MEMBER DIRECT (MD) PORTAL

We requested a demonstration of the new MD portal process from the Benefits staff for making these changes.

Test Note:

- Review Direct Deposit Change Process in MD Portal
- Review Security Features in the MD Portal
- Additional Verification – RT contact member confirming change request
- Administrative, Internet & Network Security – hosted by LRS

Recommendations

:

1. We recommend that the Benefits Department enhance its review process to strengthen fraud detection further. Specifically, if a single routing number appears in more than five direct deposit change requests within a month, staff should investigate the legitimacy of those requests immediately.
2. To enhance security, we recommend requiring members to upload a photo of their driver's license, passport, or government-issued ID when submitting a direct deposit change request through the MD portal. This is especially important for members switching to virtual-only banks (e.g., Green Dot, Chime, SoFi, etc.), as recovering misappropriated funds can be very challenging.
3. We recommend that ACERA establish a separate set of security questions that are entirely different from those used and stored in the PG or MD portal.

Conclusion:

We conducted our first fraud-related audit for reviewing direct deposit account data and are pleased to report that we found no evidence of fraudulent activity. The direct deposit account change process was deemed EFFECTIVE, and the new MD portal appeared to be functioning as designed.

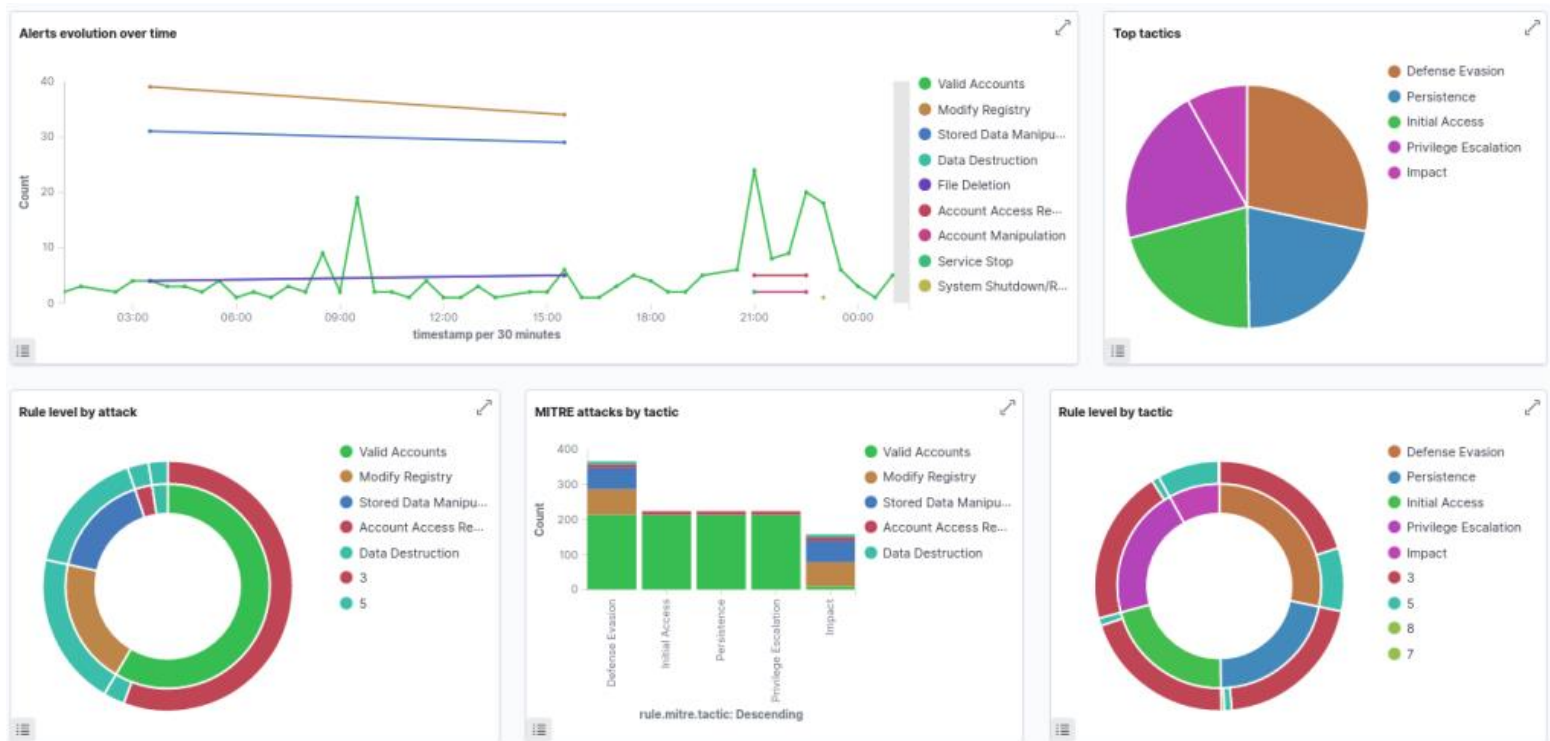
Cybersecurity Update

February 20, 2025

Vijay Jagar

Cybersecurity - Approaches

Cybersecurity Framework - NIST



Cybersecurity – 2024 in Review

- 41% increase in the number of attacks
- Email - Top malicious filetypes
 - HTML - 55%
 - PDF - 20%
 - EXE - 15%
 - web links - 5%
 - DOC - 4%
- Phishing and Social Engineering Attacks
 - Scam-farms
- Identity Theft



The Changing Threat Landscape

- Generative AI
 - phishing
 - malware development
 - deepfakes
 - vulnerability research
 - reconnaissance



The Changing Threat Landscape

US Federal Government

Geopolitical Tensions - The Big Four

- Russia
- China
 - Embedded Systems
- North Korea
 - Impersonation of remote IT workers
- Iran



Questions



MEMORANDUM TO THE AUDIT COMMITTEE

DATE: February 20, 2025

TO: Members of the Audit Committee

FROM: Harsh Jadhav, Chief of Internal Audit

SUBJECT: Results of the Member Direct Deposit Audit

Audit Objective

This audit aimed to identify any suspicious or fraudulent activities related to recent direct deposit bank account change requests. Given the evolving nature of fraud schemes and the ongoing volume of member change requests, we have implemented audit technology to allow our team to run a recurring audit on a periodic basis.

Audit Results

We are pleased to report that we found no evidence of fraudulent activity. The direct deposit account change process was deemed **EFFECTIVE**, and the new MD portal appears to be functioning as designed.

Key Findings and Recommendations

Although there were no significant findings, we made the following recommendations:

1. We recommend conducting a periodic fraud audit every three to six months, depending on the workload of the Internal Audit Department.
2. We recommend that the Benefits Department enhance its review process to strengthen fraud detection further. Specifically, if a single routing number appears in more than five direct deposit change requests within a month, staff should investigate the legitimacy of those requests immediately.
3. We recommend requiring members to upload a photo of their driver's license, passport, or government-issued ID when submitting a direct deposit change request through the MD portal.
4. We recommend that ACERA establish a separate set of security questions entirely different from those used and stored in the PG or MD portal. These security questions should be stored in a separate system, such as EDMS, to serve as an additional layer of protection.



Alameda County Employees' Retirement Association
Internal Audit Department

Member Direct Deposit (Fraud) Audit Year 2024

**AUDIT TO DISCOVER POTENTIAL FRAUDULENT ACTIVITIES ON
THE DIRECT DEPOSIT**



Auditing for Fraud:

**REPORT PREPARED FOR:
ACERA BOARD OF RETIREMENT**

TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
CONTROL SUMMARY	2
KEY CONTROLS	2
RISK LEVEL	3
CONTROL EFFECTIVENESS.....	3
EXECUTIVE SUMMARY	4
AUDIT OBJECTIVE	5
SCOPE AND STRATEGY	5
AUDIT LIMITATIONS.....	6
INTERNAL AUDIT GUIDANCE AND STANDARDS.....	6
CONTROLS TESTED.....	8
CONTROL 1 – VERIFICATION OF THE DIRECT DEPOSIT ACCOUNT CHANGE REQUEST	8
CONTROL 2 – DIRECT DEPOSIT ACCOUNT CHANGE REQUEST THROUGH MEMBER DIRECT (MD) PORTAL.....	10
CONCLUSION.....	12

CONTROL SUMMARY

KEY CONTROLS

#	Control	Risk Level	Effectiveness
1	VERIFICATION OF THE DIRECT DEPOSIT ACCOUNT CHANGE REQUEST: This control reviewed the selected samples of recent direct deposit account change requests, mainly from 2024. We examined a sample selection of monthly ACH files to detect whether any suspicious fraudulent activities were present.	Medium	Effective
2	DIRECT DEPOSIT ACCOUNT CHANGE REQUEST THROUGH MEMBER DIRECT (MD) PORTAL: This control reviewed member processes using the Member Direct (MD) portal to make changes to their direct deposit account.	Medium	Effective

RISK LEVEL

High-Risk Controls:

Controls associated with critical processes within an organization. Typically, they are related to overall monitoring controls or valued in key or numerous processes. They can be controls that had significant findings in previous years. A high-risk control failure could result in a material weakness. Material weakness includes material misstatements in the financial statements, significant process errors, and ACERA resource misuse.

Medium-Risk Controls:

Controls associated with important processes within an organization, where a deficiency in the control could cause financial loss or breakdown in process, but in most cases, do not lead to a critical systemic failure. Typically, these controls had minimal or no findings in previous years but are integral to the process and necessary to test on a regular basis. A medium-risk control failure could result in a significant deficiency and, in some instances, a material weakness. Significant deficiencies can include staff competency, lack of consistent business processes, and poor utilization of ACERA resources.

Low-Risk Controls:

Controls associated with process optimization and non-critical processes. Typically, they represent controls that did not have findings in the previous year's testing and have not changed how they operate or the personnel performing the controls. Low-risk controls are inherent in the current control environment. Still, they are unlikely to cause a material misstatement unless several low-risk controls fail within the same process.

CONTROL EFFECTIVENESS

Effective:

The control is fully operating as designed.

Partially Effective:

The control is operating as designed with the modification necessary due to a change in business process, change in personnel, inadequate documentation, the control has not been fully implemented, or the control requires additional enhancements to be effective. Often, new controls will fall into this category.

Improvement Opportunity:

The control is only marginally effective and should be redesigned or implemented. Typically, these controls require review due to an ineffective design, preventing the control from detecting control risk.

Ineffective:

If not remediated, the control is not operating as designed and could lead to a significant risk to the organization.

Remediated/In Remediation:

The control was previously ineffective, partially effective, or an improvement opportunity. A remediation plan is in place to correct the deficiency. Note that reliance can be placed on the remediated control, typically in the following audit cycle, once retested.

EXECUTIVE SUMMARY

Alameda County Employees' Retirement Association (ACERA) processes monthly pension benefits for its members primarily through direct deposit to their bank accounts (ACH). Members can set up or request direct deposit in one of three ways:

- (1) **Retirement Application Process:** Members provide banking information, such as a voided check or a bank statement, during the retirement application process.
- (2) **Direct Deposit Authorization Form:** Members can download the Direct Deposit Authorization Form from ACERA's website or request the form from the office. After signing the form, they submit it with their banking information, such as a voided check or bank statement.
- (3) **Web Member Services (WMS) or Member Direct (MD) Portal:** This newer option allows members to change their deposit bank account information through the secured MD portal. Members must have an active MD account with a login ID and password. Notably, a voided check or bank statement is no longer required when making changes through the portal.

In 2023, the Internal Audit Department launched a member authentication process survey to assess the effectiveness of security measures across all 1937 Act retirement systems. To ensure broad participation, we partnered with CALAPRS to distribute the survey. A total of 19 retirement systems responded to the 22-question survey.

The survey results revealed a new risk: some retirement systems reported incidents in which external fraudsters attempted to change the direct deposit bank account information for members receiving pension benefits. This finding highlighted a critical vulnerability that warranted further attention and action.

In response to the findings, ACERA's CEO and the Internal Audit Department partnered with CAPAPRS to present the survey results at the CALAPRS Advance Course.

We determined that the fraudulent activity usually has two major components:

- (1) Fraudsters are likely opening new bank accounts with fintech or virtual-only banks using personal information obtained from the dark web.
- (2) Fraudsters are submitting direct deposit change requests through online or member portals, enabling them to bypass a "human in the loop (HITL)" control and avoid detection.

To better assess and mitigate the risks associated with direct deposit changes, the Internal Audit Department launched a comprehensive audit—our first audit specifically focused on member fraud prevention. In addition, we leveraged advanced data analytics software to examine activities related to direct deposit change requests. In the future, this approach will help the Internal Audit Departments to proactively identify and address potential fraudulent activity, minimizing the risk of fraud-related losses.

AUDIT OBJECTIVE

The objective of this audit is to identify any suspicious or fraudulent activities related to recent direct deposit bank account change requests.

Given the evolving nature of fraud schemes and the ongoing volume of member change requests, we have implemented audit technology to allow our team to run a recurring audit on a periodic basis. This audit will serve as a valuable reference for future audits, enhancing efficiency and reducing the time required to conduct similar assessments.

SCOPE AND STRATEGY

ACERA's Internal Audit Department conducted a limited-scope audit of the Member Direct Deposit Account Change process. The scope was defined based on our understanding of the business process and an assessment of the highest-risk areas. The primary focus of this audit was to review recent member account requests involving changes to bank accounts with fintech banks and virtual-only banks, such as Green Dot Bank, Capital One, Discover, Credit Karma, etc. We also reviewed related procedures to assess the effectiveness of the current internal controls over the process.

Please note that this audit's scope did not include the network and system security for the Pension Gold (PG) system and the Member Direct (MD) user portal.

Given the known risks these institutions pose, our audit focused on accounts associated with fintech or virtual-only banks. Unlike traditional banks, these banks might lack robust internal controls and follow less rigorous methods of validating current addresses, physical identification documents or requiring an initial deposit when opening new accounts. In contrast, traditional banks with physical branches tend to have more comprehensive account opening procedures, making it more difficult for fraudsters to exploit personal information from the dark web to open fraudulent accounts.

We created a list of routing numbers used by ACERA's members to validate the banks' routing numbers by referencing certain third-party websites. Using data analytics software, we matched approximately 22,000 routing number records from two monthly ACH files (PG system version 2) against the list of bank routing numbers sourced from these third-party websites. This allowed us to identify which banks were classified as traditional, fintech, or virtual. We were concerned that some fraudsters might use a traditional bank's name on the account change form to avoid detection and route through a virtual bank's routing number.

We selected higher-risk activities for review in this audit. In ACERA's documentation database system, EDMS, we examined the signed Direct Deposit Authorization Forms submitted by members and any voided checks or banking information provided. If documentation was available, we authenticated the signature on the most recent form by comparing it with signatures on earlier documents, such as the Member Enrollment Questionnaire or Application for Service Retirement, to assess whether the signatures matched.

During this audit, in October 2024, ACERA upgraded the PG system from Version 2 to Version 3, and the Web Member Services (WMS) portal was transitioned to the newer Member Direct (MD) portal. As a result, some processes have been updated. To familiarize ourselves with the

changes, staff from the Benefits Department kindly provided a walkthrough of the direct deposit account request process in PG Version 3 and the MD portal.

The audits were performed by ACERA's Internal Audit staff, who have adequate technical training and proficiency as auditors. In all matters relating to the audit, the auditors maintained independence and objectivity. Professional care was exercised during the audit performance and the report preparation. In planning the engagement, a sufficient understanding of the internal controls was obtained to plan the audit and to determine the nature, timing, and extent of tests to be performed. Appropriately evidential matter was obtained through inspection, observation, inquiries, and confirmations to provide a reasonable basis for an audit opinion.

Furthermore, ACERA's Internal Audit Department personnel are not trained or qualified to offer legal, actuarial, or investment recommendations. Any questions on these issues should be directed to the appropriate party. Hence, no part of the Internal Audit Report should be construed as legal, actuarial, or investment advice.

AUDIT LIMITATIONS

Since the interpretation of certain law statutes required professional knowledge, to mitigate this ambiguity, the audit department solicited the assistance of ACERA's Legal and Benefits Departments to provide guidance on the intent and application of specific legislation. Due to certain resource constraints, the audit was limited in scope to focus on the highest-risk areas, which may not represent a comprehensive review of all high-risk areas.

Further, we sampled records representing the population to be efficient in the audit testing. Whenever a random sampling approach is used, a sampling risk arises from the possibility that the auditor's conclusions from testing the sample may differ from those drawn if the entire population had been tested. Finally, please note that this audit's primary purpose was not to detect payroll fraud, non-compliance with federal or state statutes, or other compliance issues outside the scope of this audit. Sometimes, during the course of an audit, new information is uncovered, or a new risk is identified, which could change our audit strategy, including potentially expanding the audit scope.

INTERNAL AUDIT GUIDANCE AND STANDARDS

Internal auditing is conducted in diverse legal and cultural environments, within organizations that vary in purpose, size, complexity, and structure, and by persons within or outside the organization. While differences may affect internal auditing practice in each environment, using the IIA's *International Standards for the Professional Practice of Internal Auditing (Standards)* and other established standards as guidelines is essential in meeting the responsibilities of internal auditors and the internal audit activity. If internal auditors or internal audit activity is prohibited by law or regulation from conforming to our role as internal auditors, appropriate disclosures are needed.

If the *Standards* are used in conjunction with standards issued by other authoritative bodies, internal audit communications may also cite the use of other standards as appropriate.

The purpose of the *Standards* is to:

- (1) Delineate basic principles that represent the practice of internal auditing.
- (2) Provide a framework for performing and promoting a broad range of value-added internal auditing.
- (3) Establish the basis for the evaluation of internal audit performance.
- (4) Foster improved organizational processes and operations.

The *Standards* are principles-focused, mandatory requirements consisting of:

- (1) Statements of basic requirements for the professional practice of internal auditing and for evaluating performance effectiveness, which are internationally applicable at organizational and individual levels.
- (2) Interpretations, which clarify terms or concepts within the Statements. The Standards employ terms that are specific. Specifically, the Standards use the word "must" to specify an unconditional requirement and the word "should" where conformance is expected unless, when applying professional judgment, circumstances justify deviation. It is necessary to consider the Statements and their Interpretations as well as the specific meanings from the Glossary to understand and apply the Standards correctly.
- (3) The structure of the *Standards* is divided between Attribute and Performance Standards. Attribute Standards address the attributes of organizations and individuals performing internal auditing. The Performance Standards describe the nature of internal auditing and provide quality criteria against which the performance of these services can be measured. The Attribute and Performance Standards are also provided and can be applied to all internal audit services.

Assurance services involve the internal auditor's objective assessment of evidence to provide an independent opinion or conclusions regarding an entity, operation, function, process, system, or other subject matter. The nature and scope of the assurance engagement are determined by the internal auditor. There are generally three parties involved in assurance services:

- (1) The person or group directly involved with the entity, operation, function, process, system, or other subject matter - the process owner.
- (2) The person or group making the assessment - the internal auditor
- (3) The person or group using the assessment - the user.

Consulting services are advisory in nature and are generally performed at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement with the engagement client. Finally, the Internal Audit Department personnel are not trained or qualified to offer legal, actuarial, or investment recommendations. Any questions on these issues should be directed to the appropriate ACERA Department or qualified consultant. Hence, no part of the Internal Audit Report should be construed as legal, actuarial, or investment advice.

CONTROLS TESTED

We reviewed the routing numbers from the April and September 2024 ACH files, each containing approximately 11,000 pension benefit payment records with their associated bank routing numbers. We verified these routing numbers against a third-party website to gather additional information, such as bank names and operating states.

Additionally, we proactively searched for known routing numbers from fintech and virtual-only banks that were not yet used by our members and added them to our list. Some of the banks included in this search were:

- Chime Bank
- Current Bank
- Cash App
- Stride Bank
- Dave Bank
- Wise App
- Credit Karma
- Brex Bank
- Green Dot Bank

We compiled a comprehensive list of over 600 routing numbers specific to ACERA membership, and we plan to regularly update this list to account for changes in member banking activity and the emergence of new financial institutions.

Using data analytics software, we matched the routing numbers from the bank institution list and the ACH files. We then selected samples primarily from the 2024 direct deposit account requests that involved switches to virtual-only banks. This approach enabled us to target higher-risk activities for further review.

CONTROL 1 – VERIFICATION OF THE DIRECT DEPOSIT ACCOUNT CHANGE REQUEST

Risk Level - Medium

Control:

This control involved reviewing selected samples of recent direct deposit account change requests, primarily from 2024. We examined selected monthly ACH files to identify potential suspicious or fraudulent activities.

Our primary focus was on requests involving changes to virtual-only banks, as we learned that fraudsters often exploit these banks to open fake accounts and carry out fraudulent activities.

For requests where the member-submitted a Direct Deposit Authorization Form, we compared the signature on the form with signatures from earlier documents to validate the authenticity of the bank account change request.

In cases where a handwritten signature was not available—such as when members used an online form with an e-signature or submitted requests through the WMS portal—we authenticated the change requests by reviewing any supporting documents, such as bank letters or identification cards, submitted alongside the request.

Risk:

As fraud cases continue to rise, organizations may face an increased risk from external fraudsters targeting companies with inadequate internal controls or weak authentication processes.

Audit Results:



Test Notes:

After reviewing the samples, we found no evidence of fraudulent activities in the 2024 direct deposit account change requests.

The signatures on the Direct Deposit Authorization Forms appeared legitimate. In several cases, we noted that the Retirement Technician (RT) had left a note indicating they contacted the member directly to verify the change request.

We also identified three ACERA members using a certain fintech/virtual bank. Given that other retirement systems had reported potentially fraudulent activity associated with that same bank, we reviewed all three members' direct deposit change requests, regardless of when the requests were submitted. In each case, the member had either provided an identification card or had been contacted by the RT to confirm the request.

Additionally, we observed another case where a high volume of change requests for switching direct deposit accounts were made. We reviewed many of these requests and found no evidence of fraudulent activity.

Recommendations	Business Owner
1. As fraud schemes constantly evolve and new banks and routing numbers are frequently added, we recommend conducting a fraud audit every three to six months, depending on the workload of the Internal Audit Department. This practice can help identify and address direct deposit fraud more promptly if it occurs.	<ul style="list-style-type: none">Internal Audit Department
2. Members who change their direct deposit bank accounts, particularly those using virtual-only banks, represent a higher risk, as recovering misappropriated funds can be more difficult. To mitigate this risk, we recommend that members submit a copy of their driver's license, passport, or other government-issued ID along with their change request.	<ul style="list-style-type: none">Benefits Department

CONTROL 2 – DIRECT DEPOSIT ACCOUNT CHANGE REQUEST THROUGH MEMBER DIRECT (MD) PORTAL

Risk Level - Medium

Control:

This control reviewed how members use the Member Direct (MD) portal to update their direct deposit accounts. We requested a demonstration of the new MD portal process from the Benefits staff for making these changes.

Additionally, we examined the security features in place to ensure proper safeguards when members update their direct deposit accounts.

Risk:

One potential risk is that an unauthorized individual could gain access to or take over a member's MD portal account.

Audit Results:



Effective

Test Notes:

Direct Deposit Change Process in MD Portal

During our review, the benefits staff demonstrated a member's process for updating their direct deposit information using the MD portal.

To initiate a bank account change within the MD portal, a member must log in using their MD portal credentials (account ID and password). Additionally, they are required to enter their existing bank account number on record to proceed with updating their banking details.

Furthermore, the new bank's routing number must already exist in the PG Version 3 database. If the routing number is not recognized, the system will prevent the change. In such cases, the member may need to contact our office and complete a Direct Deposit Authorization Form.

We noted a new security feature in PG Version 3: If a request is made to change a bank account to a certain virtual bank, the system flags the request, and staff is prompted to obtain additional information before processing the change.

Security Features in the MD Portal

When initially setting up their MD portal account, members have the option to enable two-step verification for added security. If someone attempts to access the MD portal from an unrecognized device, MD sends a verification code to a designated authenticator app. To gain access, the individual must enter the correct login ID, password, and verification code.

If two-step verification is not enabled, members must answer security questions when logging in from a new device.

During our walkthrough with Benefits staff, we reviewed these security features and found that the MD portal's security measures were functioning as intended.

Additional Verification

According to the Benefits Department, RT should contact members to confirm each direct deposit change request. Additionally, RT is required to document the confirmation within PG version 3. Since this process is new, it will be reviewed in future audits.

Administrative, Internet & Network Security

LRS Retirement Solutions, the third-party provider managing Pension Gold (PG) for ACERA, administers and hosts the MD portal.

For MD portal security, ACERA relies on LRS's firewall, which protects the MD portal. The MD portal faces risks similar to those of other internet, software applications, and network security. Please note that internet and network security were not within the scope of this audit.

Recommendations	Business Owner
<p>1. The Benefits Department has already implemented the MD portal's new security features and internal controls, as outlined above. Additionally, they now verify new or unknown routing numbers using a third-party website.</p> <p>Based on our survey, other retirement systems that experienced fraudulent activities reported a pattern where fraudsters submitted multiple direct deposit change requests simultaneously, often using the same bank routing number across different member accounts. One system, for instance, received 40 such requests at once.</p> <p>We recommend that the Benefits Department enhance its review process to strengthen fraud detection further. Specifically, if a single routing number appears in more than five direct deposit change requests within a month, staff should investigate the legitimacy of those requests immediately.</p>	<ul style="list-style-type: none">• Benefits Department
<p>2. Since fraudsters can open bank accounts using stolen personal information, simply providing a voided check may not be sufficient to verify a member's identity.</p> <p>To enhance security, we recommend requiring members to upload a photo of their driver's license, passport, or government-issued ID when submitting a direct deposit change request through the MD portal. This is especially important for members switching to virtual-only, as recovering misappropriated funds can be challenging.</p>	<ul style="list-style-type: none">• Benefits Department
<p>3. We recommend that ACERA establish a separate set of security questions that are entirely different from those used and stored in the PG or MD portal.</p>	<ul style="list-style-type: none">• Benefits Department• PRISM

These security questions should be stored in a separate system, such as EDMS, to serve as an additional layer of protection. This precautionary measure would help safeguard member accounts in the event of a security breach involving one of our third-party service provider systems.

- EDMS

CONCLUSION

We conducted our first fraud-related audit to review direct deposit account data and are pleased to report that we found no evidence of fraudulent activity. The direct deposit account change process was deemed **EFFECTIVE**, and the new MD portal appeared to be functioning as designed.

However, as fraud schemes continue to evolve and new banks and routing numbers are constantly introduced, we recommend performing this audit at regular intervals, subject to the Internal Audit Department's workload. Regular reviews could help detect and prevent direct deposit fraud more quickly if it were to occur.

Please note that this audit was limited to the areas specified in the scope section of this report. The findings, recommendations, and conclusions are based on the information available at the time of this review.

We sincerely thank the Benefits Department and all others who assisted us during the audit.