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, October 19, 2023
12:30 p.m.

LOCATION AND TELECONFERENCE

ACERA
C.G. "BUD" QUIST BOARD ROOM
475 14th Street, 10th Floor
Oakland, CA 94612-1900
Main Line: (510) 628-3000
Fax: (510) 268-9574

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.

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

COMMITTEE MEMBERS

HENRY LEVY, CHAIR	**TREASURER**
ROSS CLIPPINGER, VICE-CHAIR	**ELECTED SAFETY**
KEITH CARSON	**APPOINTED**
TARRELL GAMBLE	**APPOINTED**
KELLIE SIMON	**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, October 19, 2023

Call to Order 12:30 p.m.

Roll Call

Public Comment (Time Limit: 4 minutes per speaker)

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

None

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

Internal Audit

1. **Progress report on the Internal Audit Plan** - Harsh Jadhav

2. **Review Audits in Progress** - Harsh Jadhav

Trustee Comment

Future Discussion Items

Establishment of Next Meeting Date

TBD

ACERA

MEMORANDUM TO THE AUDIT COMMITTEE

DATE: October 19, 2023

TO: Members of the Audit Committee

FROM: Harsh Jadhav, Chief of Internal Audit

SUBJECT: Progress on the 2023 Internal Audit Program

Executive Summary

The Audit Committee meeting in October 2023 will feature a progress update on the 2023 Internal Audit Program, the results of the Member Authentication Audit, a presentation detailing a Fraud Prevention Roadmap, the first in a series of trustee education presentations, and a cybersecurity update.

The Internal Audit Department is still on track to perform three internal audits and three special projects and recently delivered the annual fraud training to ACERA team members. Two internal audits are due to begin in Q4 2023. The completion of the Death Benefit Audit was delayed due to resource limitations, but is still on track to be completed before the end of the year.

2023 Audit Schedule

Internal Audit Plan (2023)	Service Line	Assigned	Status	Q1	Q2	Q3	Q4
Death Benefit Audit	Internal Audit	Lyndon	Delayed	■	■	■	
Member Authentication Audit (Identity Theft Prevention)	Internal Audit	Caxton	Completed	■	■	■	
Workforce Resilience Audit (Critical Functions)	Internal Audit	Marlon, Dana, Lyndon	In Progress	■	■	■	■
Third-Party Service Provider Audit	Internal Audit	Lyndon	Not Started				■
Commercial Bank Internal Controls Project	Special Project	Caxton	Not Started				■
Pension Administration System Internal Controls Project	Special Project	Caxton, Dana, Lyndon	In Progress	■	■	■	■
Cybersecurity and Data Security Self-Assessment	Special Project	Vijay/Harsh	In Progress	■	■	■	■
2023 Annual Risk Assessment	Administration	Harsh	Completed	■			
2024 Annual Risk Assessment	Administration	Harsh	Not Started				■
Fraud Hotline Management	Administration	Lyndon	Continuous	■	■	■	■
Fraud Training	Administration	Lyndon/Caxton	Completed		■		

2023 Audit Program

Internal Audits

Death Benefit Audit
The objective of this audit is to review the process used for paying death benefits to beneficiaries of deceased retired members. The audit process will include both an examination of the existing procedures and a verification check to ensure members selected as part of the sample are alive and well.

Member Authentication (Prevent Member Identity Theft) Audit
This audit aims to strengthen internal fraud controls to prevent third parties from making unauthorized changes to member accounts and banking information. The examination will review the business process and explore technology solutions to enhance identity management controls.

Workforce Resilience Audit
The purpose of this review is to determine if ACERA has trained staff, backup personnel and documented procedures for their critical processes. As the pandemic continues, part of prudent business continuity planning requires organizations to ensure essential staff are identified, critical processes are fully documented and updated regularly, and backup personnel have been trained and assessed periodically.

Third-Party Service Provider Audit
This audit determines if the critical third-party service providers that manage ACERA's confidential and sensitive information (i.e., member data) have internal controls to prevent breaches, processes to manage adverse events, and adequate incident response procedures.

Special Projects

Commercial Bank Internal Controls Project
The Fiscal Services Department has asked Internal Audit to provide advisory services and test internal controls for segregation of duties as ACERA transitions to a new commercial bank to manage a suite of services, including retirement payroll, expense administration, and vendor payments.

Pension Administration System Internal Controls Project
The objective of this special project will be for the Internal Audit Department to support the business with technical guidance on risk and internal controls as the leadership plans to roll out Pension Gold (Version 3) to the organization.

Cybersecurity and Data Security Self-Assessment Project
The objective of this special project will be to work with the PRISM Department to determine if adequate firewalls, access controls, employee training, and processes for incident response, business recovery, and threat analysis are in place to ensure sensitive organizational data and member data is protected and secure.

.

Internal Audit Department 2023 Internal Audit Plan

October 19, 2023

Agenda

- Progress on the 2023 Internal Audit Plan - Harsh
- Results of the Member Authentication Audit - Caxton
- Benefits Department – Fraud Prevention Roadmap - Jessica
- Risk 101 – Trustee Education Series – Trustee Levy
- Cybersecurity Update - Vijay

2023 Internal Audit Plan

Internal Audit Plan (2023)	Service Line	Assigned	Status	Q1	Q2	Q3	Q4
Death Benefit Audit	Internal Audit	Lyndon	Delayed	🟪	🟪	🟪	
Member Authentication Audit (Identity Theft Prevention)	Internal Audit	Caxton	Completed	🟥	🟥	🟥	
Workforce Resilience Audit (Critical Functions)	Internal Audit	Marlon, Dana, Lyndon	In Progress	🟧	🟧	🟧	🟧
Third-Party Service Provider Audit	Internal Audit	Lyndon	Not Started				🟦
Commercial Bank Internal Controls Project	Special Project	Caxton	Not Started				🟪
Pension Administration System Internal Controls Project	Special Project	Caxton, Dana, Lyndon	In Progress	🟦	🟦	🟦	🟦
Cybersecurity and Data Security Self-Assessment	Special Project	Vijay/Harsh	In Progress	🟨	🟨	🟨	🟨
2023 Annual Risk Assessment	Administration	Harsh	Completed	🟩			
2024 Annual Risk Assessment	Administration	Harsh	Not Started				🟦
Fraud Hotline Management	Administration	Lyndon	Continuous	🟧	🟧	🟧	🟧
Fraud Training	Administration	Lyndon/Caxton	Completed		🟩		

Staff Contribution to the Audit Profession

- Lyndon was selected by the Association of Public Pension Fund Auditors (APPFA) to serve on the Bylaws Committee. It is an honor to be selected as a committee member, as this organization includes pension fund auditors from across the United States and Canada, including representatives from CALPERS and CalSTRS.

- As part of his Member Authentication Audit, Caxton took the initiative to develop a best practice survey on member authentication, which will be distributed through CALAPRS to their membership. Given the recent PBI breach, CALAPRS felt the data collected in this survey was important and asked Caxton and Dave to discuss the results at the Administrators Roundtable.

Member Authentication Audit

Member Authentication Audit Objective

This audit reviewed whether the Retirement Technician followed the existing procedure to authenticate the callers’ identification and only disclosed the member’s record after phone verification. We also reviewed the member account setup process in the WMS and the process of using DocuSign to examine if any authentication features are available.

Member Authentication Audit Scope of Work

ACERA’s Internal Audit Department performed a limited-scope audit of the Member Authentication process. The audit scope was based on the Internal Audit Department's understanding of the business process and areas deemed the highest risk. This audit scope focused primarily on the incoming calls through the Call Center. We randomly selected and listened to phone conversation recordings to determine whether the RT followed the standard departmental procedures by asking questions to authenticate the callers.

Member Authentication Audit Observations

Based on the available recordings, we summarized our observations as follows:

• In 79% of calls, the staff asked three or four pieces of personal information to authenticate callers;

• In 15% of calls, the staff asked for two personal information to authenticate callers;

• In 6% of calls, the staff didn’t ask for personal information. But in these cases, the member was asking a general question.

We also noted that in 12 out of 87 calls, the benefits staff asked for personal information in addition to the name, social security number, date of birth, or address to verify the caller’s identity (alternate identifier), as directed and allowed in current ACERA procedures. Asking for unique personal information is a best practice since common personal information is often available on the dark web.

Member Authentication Audit Key Recommendations

1. **Member Education**

It was alarming that 4 out of 12 members independently notified ACERA that their direct deposit bank accounts were hacked (unrelated to their business with ACERA). It may be helpful to remind our members or provide them with some training on best practices to prevent fraud.

Also, our retirement seminars, newsletter, and website can be used to inform members how ACERA usually contacts them (i.e., by U.S. mail or returning member’s phone calls) to prevent members from being scammed by potential imposters pretending to be ACERA staff.

Member Authentication Audit Key Recommendations

2. Terminated Members

For terminated members with account balances, ACERA no longer receives information updates from employers. We highly recommend that if the terminated member applies to withdraw their whole ACERA account balance, it may be more secure to ask the member to provide a copy of the driver's license with their withdrawal account balance request. The copy of the driver's license can be treated as a backup to validate the withdrawal request, especially for those with a different address from ACERA’s record or those using a virtual-only bank, i.e., Chime.

Benefit Department Comment – We are in the process of updating our term form. In addition to the need for a valid ID, requests for a refund over $1,000 must be notarized unless the member presents an ID and signs in front of the team member.

Member Authentication Audit Key Recommendations

3. **Virtual Banks**

Members changing addresses or direct deposit bank accounts, especially those using a virtual-only bank (i.e., Chime, SoFi, etc.), are higher-risk activities since recovering misappropriated funds is more challenging. We recommend that members provide a copy of their driver's license, passport, or government-issued identity card with their change request.

Member Authentication Audit Key Recommendations

4. Unique Personal Information (Alternate Identifiers)

As fraud cases continue to increase, people's personal information, such as name, social security number, address, date of birth, etc., are sold on the dark web. On top of these basic four general information, we recommend the Call Center staff ask for unique personal information to authenticate members, such as years of service credit, job title, the last department worked, or the net amount of the last retirement check from ACERA.

Benefits Department Comment – In July 2023, the policy was updated to include this. However, more identifiers can be added for more security.

Member Authentication Audit
Key Recommendations

5. **No Spouse or Work Email Accounts**

Among calls to the Call Center regarding WMS login or password reset issues, we note that members used an email account to which they no longer had access when they originally set up their WMS account. It may be beneficial to note updating the email in the WMS portal in the new account setup process and reminding members not to use their work or spouse's email to set up their WMS account during all ACERA-provided training, regular correspondence, and on the ACERA website.

Benefits Department Comment - As part of the counseling process, members are directed to update their email address from the work email to a personal email address.

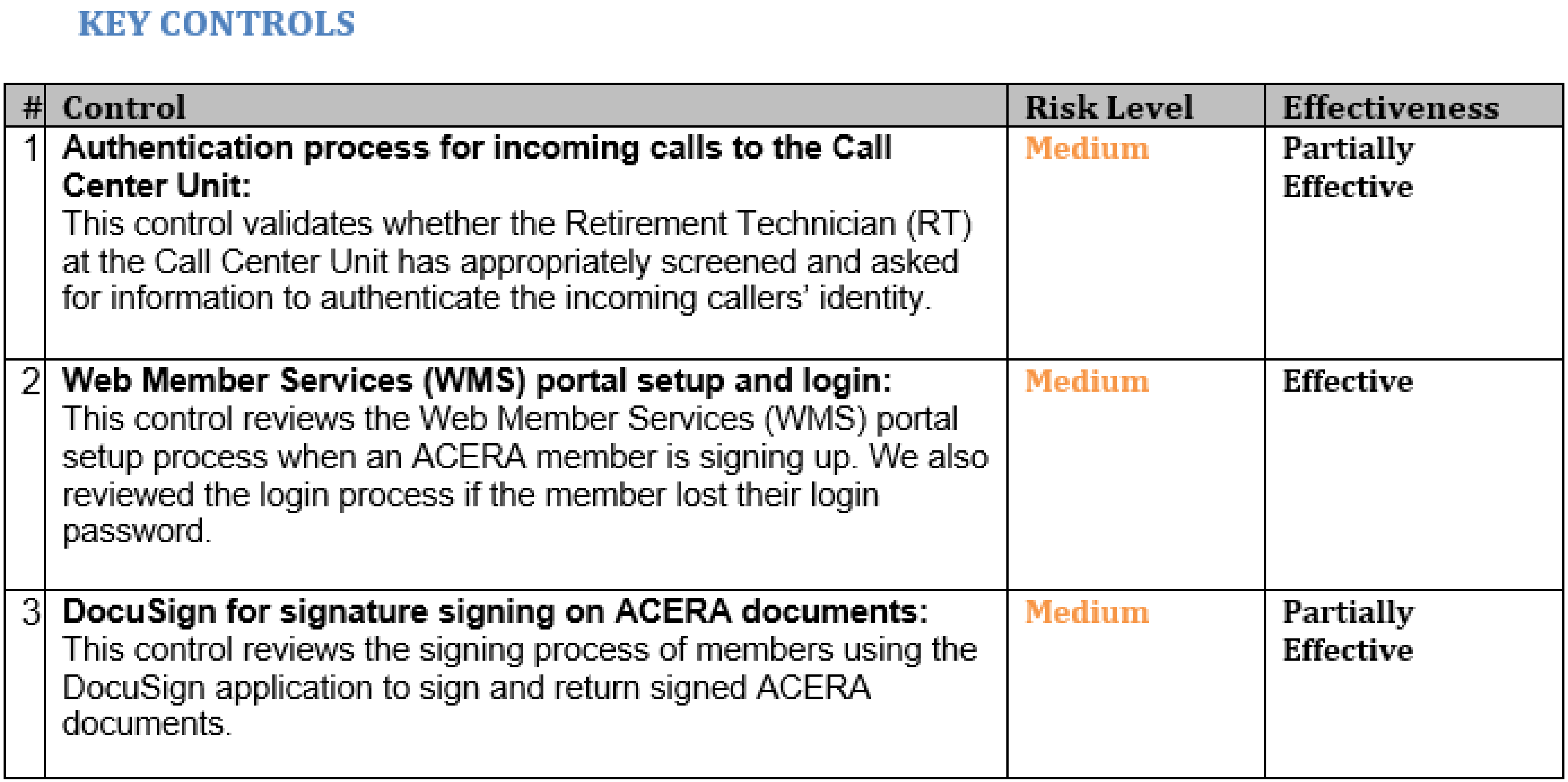
Member Authentication Audit Key Recommendations

6. **DocuSign Signature Verification**

The Benefits Department has an overall verification process validates many backup documents when a benefit request is received, including staff checking the email address where the signed form is sent for verification. However, it is sometimes difficult for a reader to tell if this particular step was performed.

We recommend singling out both the signature verification for paper-and-ink signed forms and email address verification for DocuSign signed forms as a separate checkbox (or other approval method) in the procedures for all current and future OnBase workflow Processes so staff, process verifiers, and manager would be able to tell the signature has been verified.

Member Authentication Audit Results



KEY CONTROLS

#	Control	Risk Level	Effectiveness
1	**Authentication process for incoming calls to the Call Center Unit:** This control validates whether the Retirement Technician (RT) at the Call Center Unit has appropriately screened and asked for information to authenticate the incoming callers' identity.	Medium	Partially Effective
2	**Web Member Services (WMS) portal setup and login:** This control reviews the Web Member Services (WMS) portal setup process when an ACERA member is signing up. We also reviewed the login process if the member lost their login password.	Medium	Effective
3	**DocuSign for signature signing on ACERA documents:** This control reviews the signing process of members using the DocuSign application to sign and return signed ACERA documents.	Medium	Partially Effective

Benefits Department – Fraud Prevention Roadmap

Jessica Huffman, Retirement Benefits Manager

Primary Goal

To safeguard member accounts

Areas of Focus

❑ Continuous review of internal procedures to identify and mitigate areas of risk

- Added stringent verification and authentication checks
- Shift of forms to DocuSign
- Implemented security enhancements to WMS to protect member accounts

❑ Effective collaboration with other ACERA internal departments and peers

- Heightened communication
- Sharpened use of today's technology
- Best practices
- Proactive approach for early detection

❑ Focused and ongoing training for staff and management

- ACERA's role in preventing fraud
- Fraud training workshops
- Educational courses/certificates
- Devoted time and resources

❑ Member education and enhanced communication

- Tips and email blasts
- Real-time notifications on ACERA Website

❑ Looking towards the future

- Enhanced security features in new PAS
- Role of MemberDirect and EmployerDirect
- Expanded use of Multi-Factor Authentication
- Broaden member education & use of technology

ALAMEDA COUNTY EMPLOYEES' RETIREMENT ASSOCIATION

A Pension Trust Fund of the
County of Alameda, Oakland, CA

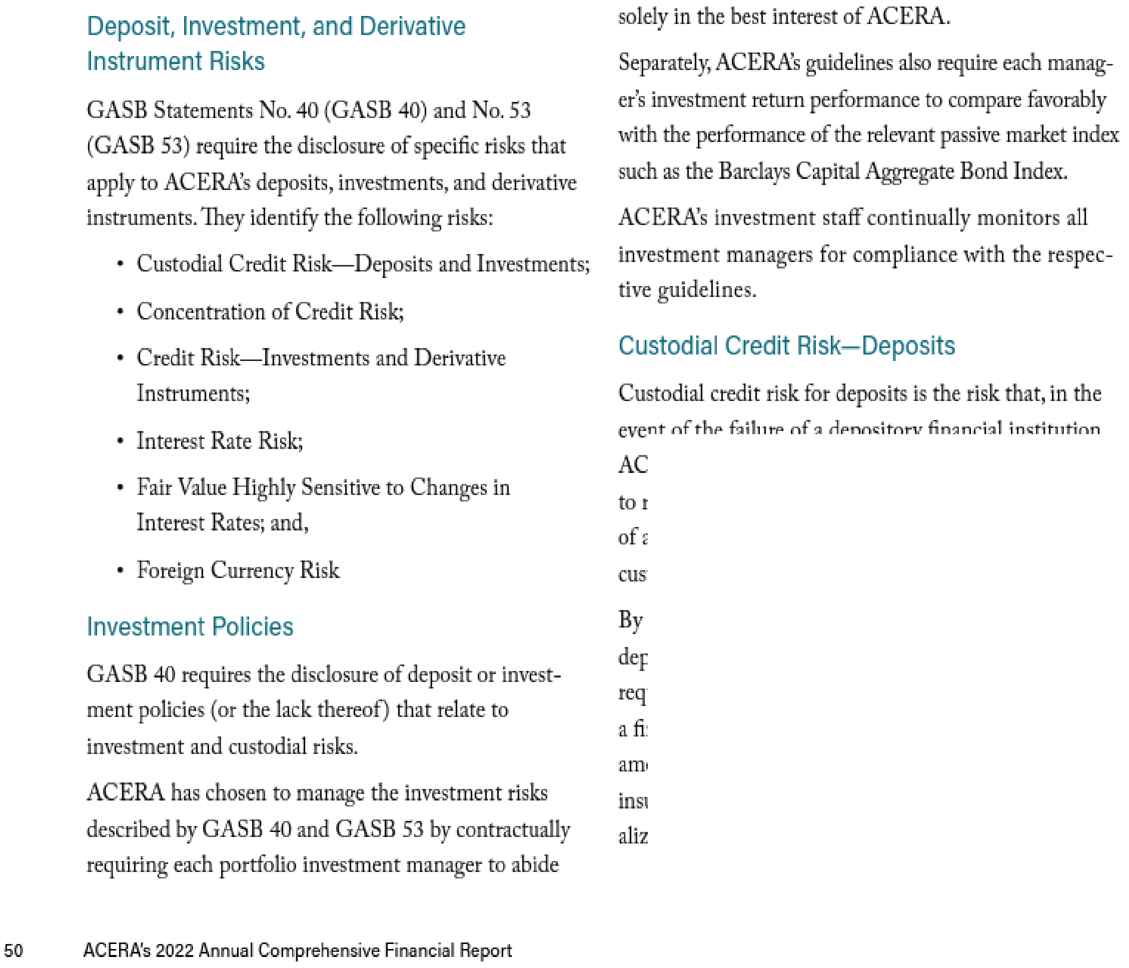
Risk 101 Trustee Education Series

Investment Policies

1. **Risk Management:** Investment policies outline the organization's risk tolerance, asset allocation strategies, and management practices. Regular reviews allow board members to assess whether these policies are still appropriate in light of changing market conditions and the organization's evolving needs.

2. **Financial Stewardship:** Board members safeguard the organization's financial resources. By regularly reviewing investment policies, they can assess the investment portfolio's performance, verify that it meets financial objectives, and make informed decisions regarding potential adjustments.

3. **Transparency and Accountability:** Transparent financial practices are crucial for maintaining trust with stakeholders, including donors, members, and the public. Regularly reviewing investment policies demonstrates the board's commitment to transparency and accountability in managing finances.



Deposit, Investment, and Derivative Instrument Risks

GASB Statements No. 40 (GASB 40) and No. 53 (GASB 53) require the disclosure of specific risks that apply to ACERA's deposits, investments, and derivative instruments. They identify the following risks:

- Custodial Credit Risk—Deposits and Investments;
- Concentration of Credit Risk;
- Credit Risk—Investments and Derivative Instruments;
- Interest Rate Risk;
- Fair Value Highly Sensitive to Changes in Interest Rates; and,
- Foreign Currency Risk

Investment Policies

GASB 40 requires the disclosure of deposit or investment policies (or the lack thereof) that relate to investment and custodial risks.

ACERA has chosen to manage the investment risks described by GASB 40 and GASB 53 by contractually requiring each portfolio investment manager to abide solely in the best interest of ACERA.

Separately, ACERA's guidelines also require each manager's investment return performance to compare favorably with the performance of the relevant passive market index such as the Barclays Capital Aggregate Bond Index.

ACERA's investment staff continually monitors all investment managers for compliance with the respective guidelines.

Custodial Credit Risk—Deposits

Custodial credit risk for deposits is the risk that, in the event of the failure of a depository financial institution

AC
to r
of a
cus

By
dep
req
a fi
am
insu
aliz

50 ACERA's 2022 Annual Comprehensive Financial Report

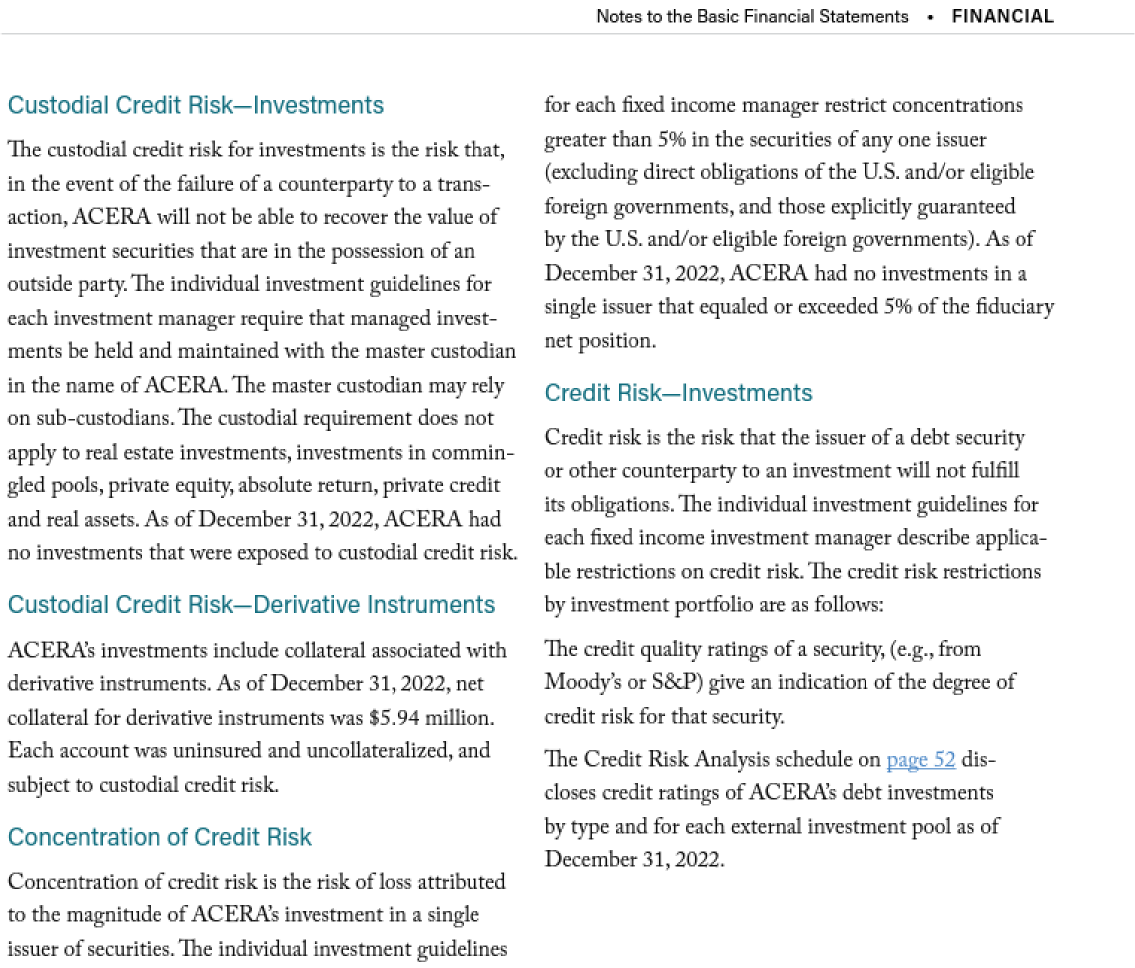
Source: 2022 Annual Comprehensive Financial Report

Credit Risk

1. **Financial Health Assessment:** Reviewing credit risks allows board members to assess the organization's financial health. By understanding the credit risk exposure, they can make informed decisions to protect the organization's financial stability and long-term sustainability.

2. **Mitigation of Default Risk:** Board members must manage default risk, especially when the organization has outstanding loans or credit agreements. Regular reviews of credit risks help identify potential issues early and enable proactive measures to mitigate the risk of default, such as renegotiating terms or securing additional financing.

3. **Compliance and Reporting:** Board members have a duty to ensure the organization complies with its financial obligations, including debt repayment. Reviewing credit risks ensures that the organization complies with loan covenants and reporting requirements, reducing the risk of penalties, legal disputes, and damage to the organization's reputation.



Notes to the Basic Financial Statements • FINANCIAL

Custodial Credit Risk—Investments

The custodial credit risk for investments is the risk that, in the event of the failure of a counterparty to a transaction, ACERA will not be able to recover the value of investment securities that are in the possession of an outside party. The individual investment guidelines for each investment manager require that managed investments be held and maintained with the master custodian in the name of ACERA. The master custodian may rely on sub-custodians. The custodial requirement does not apply to real estate investments, investments in commingled pools, private equity, absolute return, private credit and real assets. As of December 31, 2022, ACERA had no investments that were exposed to custodial credit risk.

Custodial Credit Risk—Derivative Instruments

ACERA's investments include collateral associated with derivative instruments. As of December 31, 2022, net collateral for derivative instruments was $5.94 million. Each account was uninsured and uncollateralized, and subject to custodial credit risk.

Concentration of Credit Risk

Concentration of credit risk is the risk of loss attributed to the magnitude of ACERA's investment in a single issuer of securities. The individual investment guidelines for each fixed income manager restrict concentrations greater than 5% in the securities of any one issuer (excluding direct obligations of the U.S. and/or eligible foreign governments, and those explicitly guaranteed by the U.S. and/or eligible foreign governments). As of December 31, 2022, ACERA had no investments in a single issuer that equaled or exceeded 5% of the fiduciary net position.

Credit Risk—Investments

Credit risk is the risk that the issuer of a debt security or other counterparty to an investment will not fulfill its obligations. The individual investment guidelines for each fixed income investment manager describe applicable restrictions on credit risk. The credit risk restrictions by investment portfolio are as follows:

The credit quality ratings of a security, (e.g., from Moody's or S&P) give an indication of the degree of credit risk for that security.

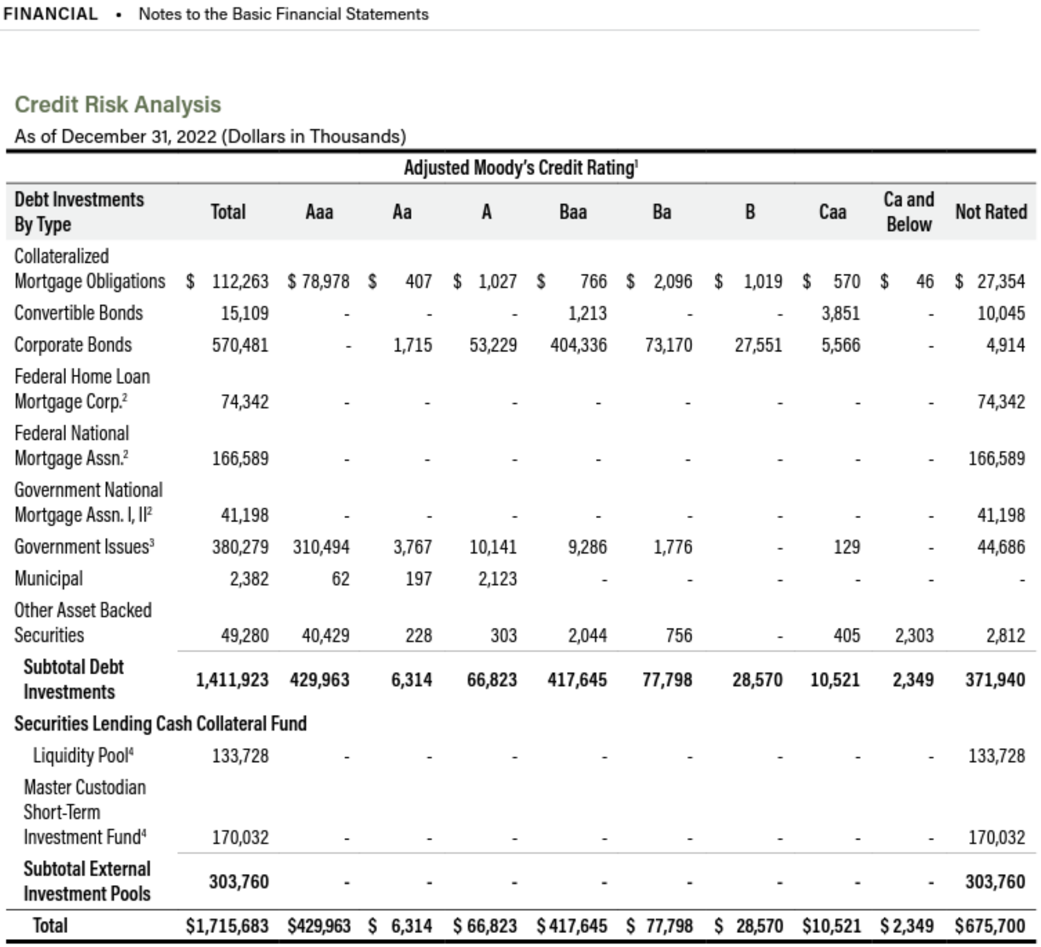
The Credit Risk Analysis schedule on page 52 discloses credit ratings of ACERA's debt investments by type and for each external investment pool as of December 31, 2022.

Importance of the Credit Risk Analysis

1. Risk Assessment: The primary purpose of credit risk analysis is to assess the potential risk associated with extending credit to a borrower or counterparty. It involves evaluating the borrower's ability and willingness to repay debt, crucial for making informed lending or investment decisions.

2. Portfolio Management: Credit risk analysis helps financial institutions and investors manage their credit portfolios effectively. By analyzing the creditworthiness of individual borrowers or issuers, organizations can diversify their portfolios, set appropriate risk appetite, and make allocation decisions that align with their risk tolerance and financial objectives.

3. Loss Prevention: Credit risk analysis is vital in preventing financial losses. By identifying high-risk borrowers or counterparties, organizations can implement risk mitigation strategies, such as requiring collateral, adjusting interest rates, or setting aside provisions for potential defaults, to reduce the likelihood and impact of credit losses



FINANCIAL • Notes to the Basic Financial Statements

Credit Risk Analysis

As of December 31, 2022 (Dollars in Thousands)

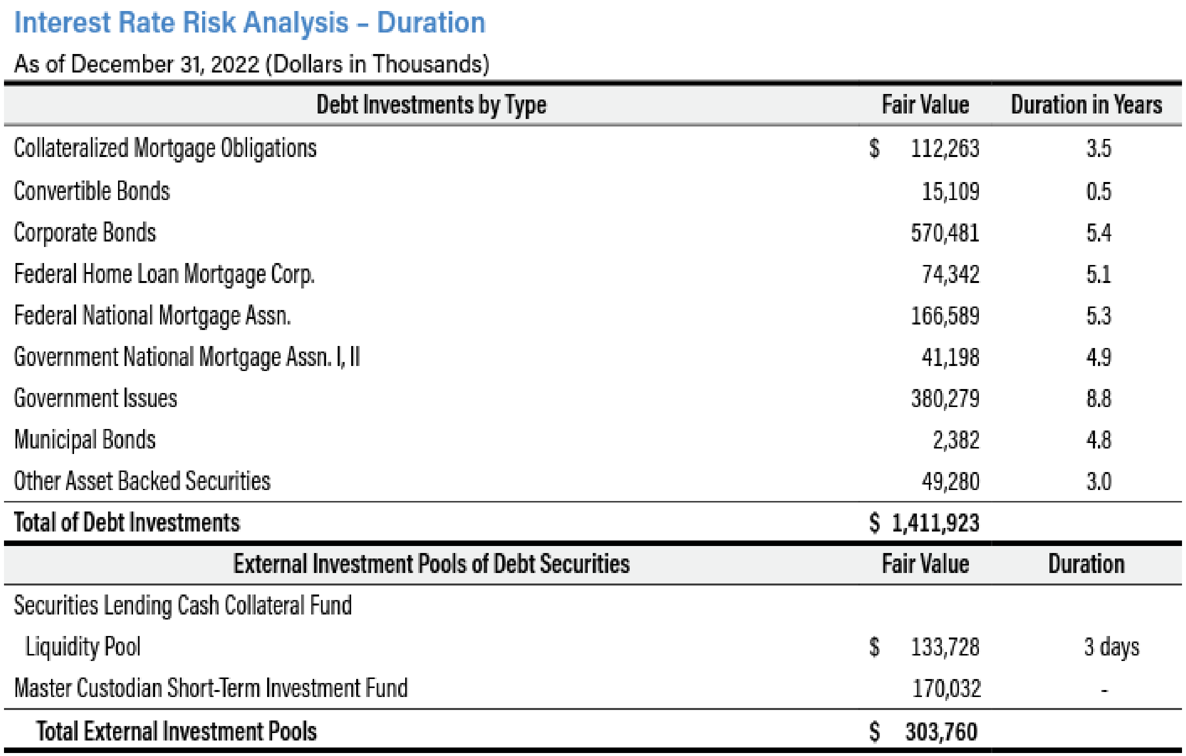
		Adjusted Moody's Credit Rating[1]								
Debt Investments By Type	**Total**	**Aaa**	**Aa**	**A**	**Baa**	**Ba**	**B**	**Caa**	**Ca and Below**	**Not Rated**
Collateralized Mortgage Obligations	$ 112,263	$ 78,978	$ 407	$ 1,027	$ 766	$ 2,096	$ 1,019	$ 570	$ 46	$ 27,354
Convertible Bonds	15,109	-	-	-	1,213	-	-	3,851	-	10,045
Corporate Bonds	570,481	-	1,715	53,229	404,336	73,170	27,551	5,566	-	4,914
Federal Home Loan Mortgage Corp.[2]	74,342	-	-	-	-	-	-	-	-	74,342
Federal National Mortgage Assn.[2]	166,589	-	-	-	-	-	-	-	-	166,589
Government National Mortgage Assn. I, II[2]	41,198	-	-	-	-	-	-	-	-	41,198
Government Issues[3]	380,279	310,494	3,767	10,141	9,286	1,776	-	129	-	44,686
Municipal	2,382	62	197	2,123	-	-	-	-	-	-
Other Asset Backed Securities	49,280	40,429	228	303	2,044	756	-	405	2,303	2,812
Subtotal Debt Investments	**1,411,923**	**429,963**	**6,314**	**66,823**	**417,645**	**77,798**	**28,570**	**10,521**	**2,349**	**371,940**
Securities Lending Cash Collateral Fund										
Liquidity Pool[4]	133,728	-	-	-	-	-	-	-	-	133,728
Master Custodian Short-Term Investment Fund[4]	170,032	-	-	-	-	-	-	-	-	170,032
Subtotal External Investment Pools	**303,760**	-	-	-	-	-	-	-	-	**303,760**
Total	**$1,715,683**	**$429,963**	**$ 6,314**	**$ 66,823**	**$ 417,645**	**$ 77,798**	**$ 28,570**	**$10,521**	**$ 2,349**	**$675,700**

Interest Rate Risk

1. **Financial Stability and Long-Term Viability:** Board members ensure the organization's financial stability and long-term viability. Reviewing interest rate risk helps them assess how fluctuations in interest rates may impact the organization's cash flows, profitability, and ability to meet financial obligations over time.

2. **Optimizing Financial Strategies:** Interest rate risk analysis allows board members to evaluate the organization's current debt structure and financial strategies. By understanding how changes in interest rates affect borrowing costs and investment returns, they can make informed decisions about refinancing debt, adjusting investment portfolios, or implementing hedging strategies to optimize financial performance.

3. **Compliance and Reporting:**. Board members need to review interest rate risk to ensure that the organization remains in compliance with these regulations and that accurate and timely reporting is provided to regulatory authorities, shareholders, and other stakeholders. Failure to do so can result in legal and reputational risks.



Interest Rate Risk Analysis – Duration

As of December 31, 2022 (Dollars in Thousands)

Debt Investments by Type	Fair Value	Duration in Years
Collateralized Mortgage Obligations	$ 112,263	3.5
Convertible Bonds	15,109	0.5
Corporate Bonds	570,481	5.4
Federal Home Loan Mortgage Corp.	74,342	5.1
Federal National Mortgage Assn.	166,589	5.3
Government National Mortgage Assn. I, II	41,198	4.9
Government Issues	380,279	8.8
Municipal Bonds	2,382	4.8
Other Asset Backed Securities	49,280	3.0
Total of Debt Investments	**$ 1,411,923**	
External Investment Pools of Debt Securities	**Fair Value**	**Duration**
Securities Lending Cash Collateral Fund		
Liquidity Pool	$ 133,728	3 days
Master Custodian Short-Term Investment Fund	170,032	-
Total External Investment Pools	**$ 303,760**	

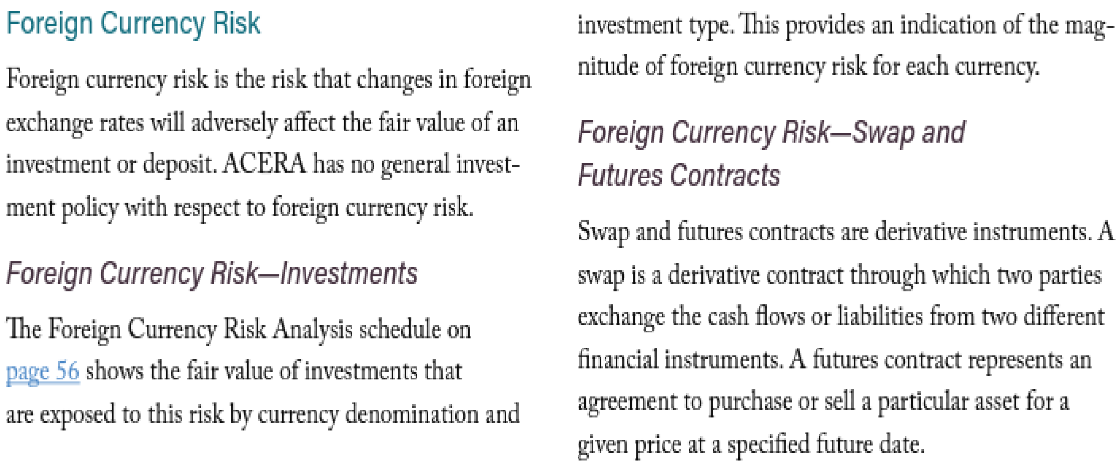
Source: 2022 Annual Comprehensive Financial Report

Foreign Currency Risk

1.Protecting Financial Stability: Reviewing foreign currency risk is essential for board members to safeguard the organization's financial stability. Fluctuations in exchange rates can significantly impact the value of assets, liabilities, and cash flows denominated in foreign currencies. By assessing and managing this risk, board members can prevent unexpected financial losses and maintain the organization's long-term viability.

2.Global Expansion and Operations: Many organizations operate globally or trade internationally. Board members must review foreign currency risk to assess the potential impact on the organization's profitability, competitiveness, and ability to expand into new markets. Effective risk management strategies, such as hedging, can help mitigate the adverse effects of currency fluctuations.

3.Compliance and Reporting: Compliance with accounting standards and regulatory requirements related to foreign currency risk is crucial. Board members must ensure that the organization follows proper accounting practices for foreign currency transactions and accurately reports the impact of currency risk in financial statements. Failure to do so can result in compliance issues and challenges in financial reporting.



Foreign Currency Risk

Foreign currency risk is the risk that changes in foreign exchange rates will adversely affect the fair value of an investment or deposit. ACERA has no general investment policy with respect to foreign currency risk.

Foreign Currency Risk—Investments

The Foreign Currency Risk Analysis schedule on page 56 shows the fair value of investments that are exposed to this risk by currency denomination and investment type. This provides an indication of the magnitude of foreign currency risk for each currency.

Foreign Currency Risk—Swap and Futures Contracts

Swap and futures contracts are derivative instruments. A swap is a derivative contract through which two parties exchange the cash flows or liabilities from two different financial instruments. A futures contract represents an agreement to purchase or sell a particular asset for a given price at a specified future date.

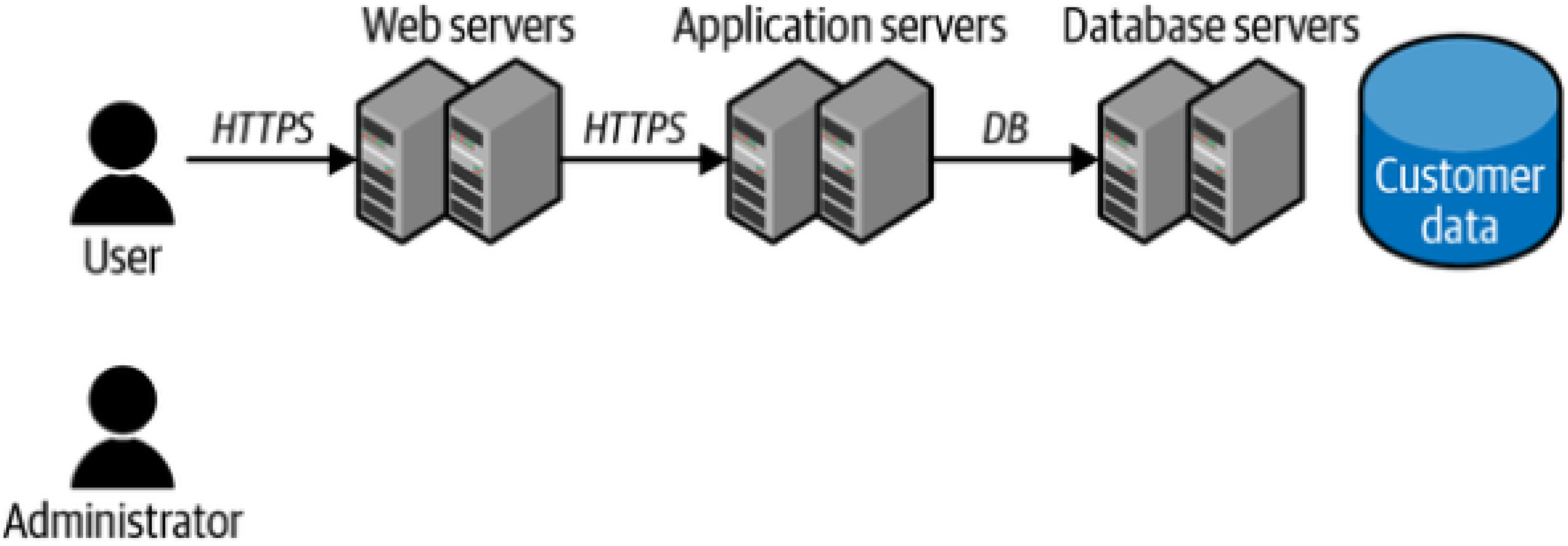
Source: 2022 Annual Comprehensive Financial Report

ACERA
www.acera.org

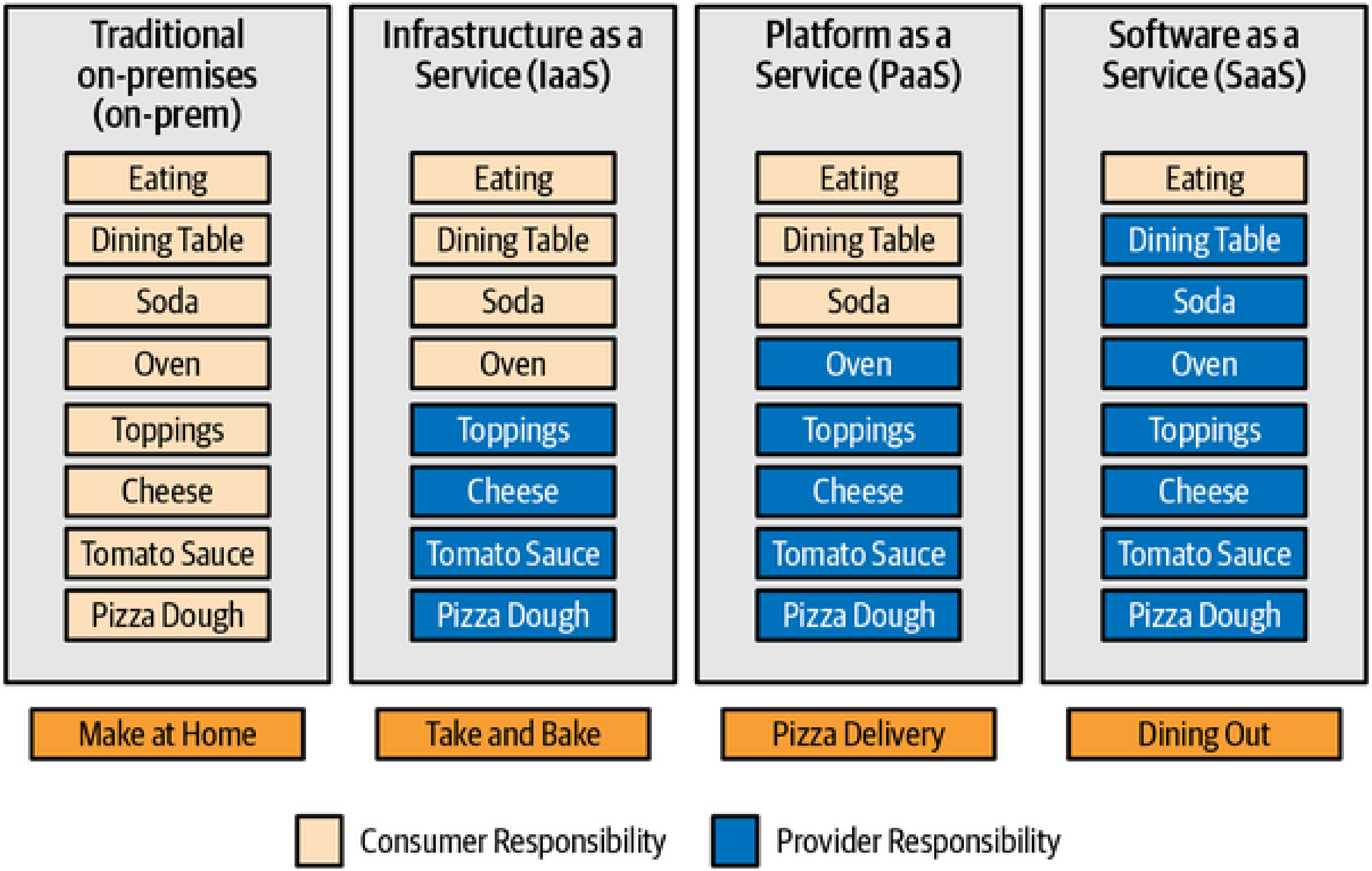
Cybersecurity Update

October 19, 2023
Vijay Jagar

Cybersecurity Update: Cloud Security



Cybersecurity Update: Cloud Security



Traditional on-premises (on-prem)	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
☐ Eating	☐ Eating	☐ Eating	☐ Eating
☐ Dining Table	☐ Dining Table	☐ Dining Table	🟦 Dining Table
☐ Soda	☐ Soda	☐ Soda	🟦 Soda
☐ Oven	☐ Oven	🟦 Oven	🟦 Oven
☐ Toppings	🟦 Toppings	🟦 Toppings	🟦 Toppings
☐ Cheese	🟦 Cheese	🟦 Cheese	🟦 Cheese
☐ Tomato Sauce	🟦 Tomato Sauce	🟦 Tomato Sauce	🟦 Tomato Sauce
☐ Pizza Dough	🟦 Pizza Dough	🟦 Pizza Dough	🟦 Pizza Dough
Make at Home	Take and Bake	Pizza Delivery	Dining Out

☐ Consumer Responsibility 🟦 Provider Responsibility

From Practical Cloud Security, 2nd Edition by Chris Dotson

Cybersecurity Update: Cloud Security

1. Least Privilege
2. Defense in Depth
3. Zero (Implicit) Trust
4. Threat Modeling

Questions

ACERA

MEMORANDUM TO THE AUDIT COMMITTEE

DATE: October 19, 2023

TO: Members of the Audit Committee

FROM: Harsh Jadhav, Chief of Internal Audit

SUBJECT: Results of the Member Authentication Audit

EXECUTIVE SUMMARY

Alameda County Employees' Retirement Association (ACERA) receives more than sixteen thousand incoming calls for benefits inquiries in a year. The Internal Audit Department performed an audit to review and assess ACERA's current member authentication processes for incoming calls through the Call Center.

AUDIT OBJECTIVE

This audit reviewed whether the Retirement Technician (RT) followed the existing procedure to authenticate the callers' identification and only disclosed the member's record after phone verification. We also reviewed the member account setup process in the WMS and the process of using DocuSign to examine if any authentication features are available.

KEY OBSERVATIONS

Based on the available recordings, we summarized our observations as follows:

- In 79% of the calls, the staff asked for three or four pieces of personal information to authenticate callers.
- In 15% of the calls, the staff asked for two personal information to authenticate callers.
- In 6% of the calls, the staff didn't ask for personal information. But in these cases, the member was asking a general question.

We also noted that in 12 out of 87 calls, the benefits staff asked for personal information in addition to the name, social security number, date of birth, or address to verify the caller's identity (alternate identifier), as directed and allowed in current ACERA procedures. Asking for unique personal information is a best practice since common personal information is often available on the dark web.

KEY RECOMMENDATIONS

1. **Member Education**
   It was alarming that 4 out of 12 members independently notified ACERA that their direct deposit bank accounts were hacked (unrelated to their business with ACERA). It may be helpful to remind our members or provide them with some training on best practices to prevent fraud. Also, our retirement seminars, newsletter, and website can

be used to inform members how ACERA usually contacts them (i.e., by U.S. mail or returning member's phone calls) to prevent members from being scammed by potential imposters pretending to be ACERA staff.

2. **Terminated Members**
   For terminated members with account balances, ACERA no longer receives information updates from employers. We highly recommend that if the terminated member applies to withdraw their whole ACERA account balance, it may be more secure to ask the member to provide a copy of the driver's license with their withdrawal account balance request. The copy of the driver's license can be treated as a backup to validate the withdrawal request, especially for those with a different address from ACERA's record or those using a virtual-only bank (i.e., Chime.)

3. **Virtual Banks**
   Members changing addresses or direct deposit bank accounts, especially those using a virtual-only bank (i.e., Chime, SoFi, etc.), are higher-risk activities since recovering misappropriated funds is more challenging. We recommend that members provide a copy of their driver's license, passport, or government-issued identity card with their change request.

4. **Unique Personal Information (Alternate Identifiers)**
   As fraud cases continue to increase, people's personal information, such as name, social security number, address, date of birth, etc., are sold on the dark web. On top of these basic four general information, we recommend the Call Center staff ask for unique personal information to authenticate members, such as years of service credit, job title, the last department worked, or the net amount of the last retirement check from ACERA.

5. **No Spouse or Work Email Accounts**
   Among calls to the Call Center regarding WMS login or password reset issues, we note that members used an email account to which they no longer had access when they originally set up their WMS account. It may be beneficial to note updating the email in the WMS portal in the new account setup process and reminding members not to use their work or spouse's email to set up their WMS account during all ACERA-provided training, regular correspondence, and on the ACERA website.

6. **DocuSign Signature Verification**
   The Benefits Department has an overall verification process validates many backup documents when a benefit request is received, including staff checking the email address where the signed form is sent for verification. However, it is sometimes difficult for a reader to tell if this particular step was performed. We recommend singling out both the signature verification for paper-and-ink signed forms and email address verification for DocuSign signed forms as a separate checkbox (or other approval method) in the procedures for all current and future OnBase workflow Processes so staff, process verifiers, and manager would be able to tell the signature has been verified.

SUMMARY

In summary, we deemed the authentication process. as Partially Effective. It should be noted that the Benefits Department was already in the process of implementing several recommendations and updating the authentication procedures and documentation to increase security for the members and ACERA. Therefore, many audit recommendations have already been addressed.

Alameda County Employees' Retirement Association
Internal Audit Department

Member Authentication Audit Year 2023

AUDIT TO REVIEW INTERNAL CONTROLS ON THE MEMBER AUTHENTICATION PROCESSES

REPORT PREPARED FOR:

ACERA BOARD OF RETIREMENT

TABLE OF CONTENTS

CONTROL SUMMARY

KEY CONTROLS

#	Control	Risk Level	Effectiveness
1	**Authentication process for incoming calls to the Call Center Unit:** This control validates whether the Retirement Technician (RT) at the Call Center Unit has appropriately screened and asked for information to authenticate the incoming callers' identity.	**Medium**	**Partially Effective**
2	**Web Member Services (WMS) portal setup and login:** This control reviews the Web Member Services (WMS) portal setup process when an ACERA member is signing up. We also reviewed the login process if the member lost their login password.	**Medium**	**Effective**
3	**DocuSign for signature signing on ACERA documents:** This control reviews the signing process of members using the DocuSign application to sign and return signed ACERA documents.	**Medium**	**Partially 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) receives more than sixteen thousand incoming calls for benefits inquiries in a year. The Internal Audit Department performed an audit to review and assess ACERA's current member authentication processes for incoming calls through the Call Center.

According to best practice, strong authentication enhances internal controls to ensure that only authorized personnel can access company systems, applications, and confidential data. This aids in protecting internal resources, preventing outsider threats, and the general security of the organization.

Based on discussion with the Benefits Department, we understand that ACERA members may contact our office and make requests through one or more of the following methods:

(1) Phone calls (8x8);
(2) Web Member Services (WMS);
(3) In-person;
(4) Fax;
(5) Email;
(6) Regular mail.

Each contact method above may require the Retirement Technician (RT) to screen our members for their identity with a unique authentication process.

After discussion with the benefits management team, reviewing the related benefits procedure(s), and considering changes to the business process with remote work, the internal audit staff performed an audit on the incoming calls through the Call Center, the setup process for the Web Member Services (WMS), and the set up process of using the DocuSign application (the document signing process).

AUDIT OBJECTIVE

This audit reviewed whether the RT followed the existing procedure to authenticate the callers' identification and only disclosed the member's record after phone verification. We also reviewed the member account setup process in the WMS and the process of using DocuSign to examine if any authentication features are available.

SCOPE AND STRATEGY

ACERA's Internal Audit Department performed a limited-scope audit of the Member Authentication process. The audit scope was based on the Internal Audit Department's understanding of the business process and areas deemed the highest risk. This audit scope focused primarily on the incoming calls through the Call Center. We randomly selected and listened to phone conversation recordings to determine whether the RT followed the standard departmental procedures by asking questions to authenticate the callers.

We also interviewed benefits staff to understand the member account setup process for the WMS and the use of the DocuSign application. The member requests through in-person, email, regular mail, fax, and portal network security were not included in this round of the audit.

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, independence and objectivity were maintained by the auditor or auditors. Due professional care was exercised in the Audit performance and the report's 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.

INSTITUTE OF INTERNAL AUDITORS (IIA) 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, conformance with The IIA's *International Standards for the Professional Practice of Internal Auditing (Standards)* is essential in meeting the responsibilities of internal auditors and the internal audit activity. If internal auditors or the internal audit activity is prohibited by law or regulation from conformance with certain parts of the *Standards*, conformance with all other parts and 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. In such a case, if inconsistencies exist between the *Standards* and other standards, internal auditors and the internal audit activity must conform to them and may conform with the other standards if they are more restrictive.

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 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 specific terms. 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 to apply 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 randomly sampled and selected phone conversation recordings between January 1, 2023, and March 28, 2023. The incoming calls came through the ACERA Call Center Unit. We selected sample recordings for the following types of inquiries and change requests:

Mario to review the subjects -

- Beneficiary
- Benefits
- Change address
- Check
- Contributions
- Death
- Direct deposit
- Disability
- Divorce
- Enrollment
- Garnishment
- Other
- Power of Attorney
- Reciprocity
- Retirement
- Rollovers
- Separate/Terminate
- Taxes
- WMS log ID
- WMS password
- WMS personal data

We listened to recordings to determine if staff authenticated callers for their identity in accordance with the Benefits Department's policies.

Since the audit department could not access the WMS and DocuSign applications, we consulted with the Benefits Department staff to explain and show us the screens of the setup processes for both applications.

CONTROL 1 – AUTHENTICATION PROCESS FOR INCOMING CALLS TO CALL CENTER UNIT

Risk Level - Medium

Control:
Most benefit requests from members to ACERA were first handled through the Call Center. This control reviewed the draft written procedures for the Benefits Department Call Center Unit regarding member authentication. In addition, we randomly selected conversation recordings from outside callers to the Call Center from January 1, 2023, to March 28, 2023. We listened to the types of information benefits staff used to validate the caller's identification.

Risk:
As fraud cases increase, organizations like ACERA may face a higher risk than before from fraudsters or dishonest relatives trying to obtain the members' personal information or scams for financial gain. It would also increase ACERA's exposure to media risk.

Audit Results:

△ Partially Effective

Test Notes:
According to the Benefits Department's draft version of the "Release of Information and Member ID Policies Supplemental" document, there were pertinent sections:

1) General information about ACERA's forms, policies, topics/events found on the website, processing timelines, monthly check date (i.e., last business day of the month), how to submit items to ACERA, office location, identification not needed.

2) Ways to Positively Identify Member Calling ACERA – Gather member's full name and DOB, plus any two personal information data points from …" There were 17 different pieces of information the Call Center staff could ask the callers for verification.

We requested 91 sample Call Center recordings from the Benefits Department, and the Benefits Department provided 87 recordings for our review.

In discussion with the Benefits Department about the situation, the benefits team has provided the reason is due to system limitations. ACERA uses two separate tracking systems, Call Center Tracking Log and 8x8 Contact Center when logging and reviewing member calls received through our Call Center. The first tracking system, Call Center Tracking Log, is a tracking Access database where ACERA Call Center agents manually enter the record of the call by member name, social security number, and reason for the call.

The database gives each call entry a tracking number, and the entry date and time are recorded after the staff login. The Call Center Tracking Log records when and why a member calls ACERA. Data from this log is also used to obtain stats on reasons why members contact ACERA. This tracking database is independent of our phone system and will not automatically note the time or date of the call as the call comes in.

The second tracking system, 8x8 Contact Center, has a call recording function where a digital recording of the call is available for playback. Recordings are stored and indexed by phone number and call date/time. The member name, Call Center Tracking Log database tracking number, and the call reason are unavailable or tracked in the 8x8 Contact Center.

Call Center agents are trained to enter the record of the member call in the Call Center Tracking Log directly after the call is completed. At times, Call Center agents cannot enter the information into the call log when the call is received due to call volume. Since the Call Center Tracking Log does not record call dates and times, it can be hard to cross-reference and locate specific calls in our 8x8 Contact Center recordings.

<u>*Summary Of Audit Findings:*</u>
Based on the available recordings, we summarized our observations as follows:

- In 79% of calls, the staff asked three or four pieces of personal information to authenticate callers;
- In 15% of calls, the staff asked two personal information to authenticate callers (13 calls);
- In 6% of calls, the staff asked none in general question situations;
- In 12 out of 87 calls, staff only asked for personal information other than name, social security number, date of birth, or address to verify the callers' identity as directed and allowed in current ACERA procedures.

We focused on how many and what types of information the Call Center staff asked the callers to authenticate their identity as part of the member authentication process.

Based on the sample recordings, we found that in most of the calls (69 out of 87, approximately 79%), staff had asked three or four questions, such as member name, social security number, date of birth, address, or other, to authenticate caller's identity. This was allowed in accordance with ACERA's policy and was not a deviation from set procedure.

In about 13 out of 87 recordings, Call Center staff had asked the callers two questions to authenticate their identity. In about 5 out of 87 recordings, Call Center staff had asked the callers no questions to authenticate their identity.

- 8/18 calls were Member inquiries / ID Taken
- 5/18 calls were General / ID Taken
- 5/18 calls were General Calls / No ID taken

In five recordings, staff did not ask for any information from callers. However, only general information, like ACERA forms to be used, was given to the callers. Or, the staff did not provide any information but re-directed the callers to the ACERA website to fill out some forms for their requests, which was allowed by the benefits department procedure.

We saw a difference in how many personal questions the Call Center staff used to authenticate the callers. The conversation could change and get complicated quickly, from general inquiries for the ACERA forms to inquiring about their retirement account information. It might be more practical to authenticate all members, even for form inquiries, to reduce the chances of staff missing positively identifying members. For example, many financial institutions have a best practice of starting with a series of identifying questions at the beginning of each call before answering a customer's general or specific question.

Benefits Department Comments –

> "Call Center staff handled calls based on the policies in effect at that time. In March 2023 and again in July 2023, the Benefits Department has independently modified internal authentication policies to require additional authentication questions. And the call sampling used by Internal Audit encompassed periods before and after the policy change. The difference could be due to updated policies that took place during the internal audit review period."

In many recordings, the callers were unclear or did not know how to initiate certain benefit processes. These inquiries could confuse Call Center staff regarding whether they should authenticate the callers since, many times, the member would need to complete certain ACERA forms for their benefits-related requests. Sometimes, the member's inquiry might originally appear to be general in nature and not require authentication. Then, additional inquiries were made during the conversation, which should require further authentication. According to the Benefits Department, the Call Center agent is required to then ask authentication questions if a call moves from a general inquiry to member-specific questions. We recommend that the Benefits Department consider changing the procedures to have Call Center staff authenticate all callers regardless of inquiry at the beginning of the call. This will reduce the risk of failing to authenticate the caller if the conversation shifts to the caller requesting more member-specific information.

We had another observation. Among the 87 recordings, only in twelve cases did staff ask for information other than the member's name, social security number, address, or date of birth to verify the callers. There are seventeen other less common pieces of information that can be used to authenticate the member listed in the procedure document, of which only a few staff chose to utilize to verify callers.

Benefits Department Comments –

> "Benefits updated their policy in July 2023 to include an alternate identifier requirement. Additional authenticators other than name, social security number, date of birth, or address are now required. Additional updates were made to the policy in July 2023, adding another layer of security when identifying members."

Summary of Audit Observations:

- Four callers out of 12 calls were related to "Direct Deposit" questions shared with ACERA staff. The members shared with Benefits Staff that they had independently experienced their bank accounts being hacked. In one case, the caller previously contacted ACERA to change his direct deposit bank account. However, his new bank account was hacked in less than a month, so he needed to make another change request. Note that none of these compromises were not related to any business with ACERA.

- One common reason members had trouble resetting their WMS password was that they used their work email or ex-spouse’s email address, which they could no longer access.

Although not part of the audit scope, we informed ACERA management about these observations.

Benefits Department Comments –

> “In all calls, the team handled them appropriately. This just demonstrates and reflects the amount of fraud outside of ACERA that members can face.”
>
> “As part of the counseling process, members are directed to update their email address from the work email to a personal email address.”

These items above are external and not in ACERA’s control. However, these observations can be used to strengthen policies, and we also recommend providing more education to members about fraud and protecting their private information.

We also consulted with the Benefits Department about the phone recording system and any available retention policy. The Call Center was using a platform from a vendor called “8 x 8 contact center”, in which all calls received through the contact center were recorded. The recordings were only accessed by leads/management for quality assurance review and were not uploaded to member files. Members were told, “When calling ACERA, calls may be monitored for training purposes.”

According to the Benefits Department, ACERA does not have an electronic records policy that would include the retention of calls or media files. Previously, there was no record retention schedule for holding saved calls, and ACERA would hold Call Center recordings based on 8x8’s storage limit. PRISM Department recently provided an update about the recordings retention period: starting from June 2023, the calls are stored for 30 days in a “Hot Storage,” which is like the real-time data for easy access and faster retrieval, and then move to “Cold Storage” as archival data for 365 days.

Recommendations	Business Owner
1. It is alarming that 4 out of 12 members called to change their direct deposit bank accounts because they were hacked. It may be helpful to remind our members or provide them with some training on best practices to prevent fraud. Also, our retirement seminars, newsletter, and website can be used to inform members how ACERA usually contacts them (i.e., by U.S. mail or returning member’s phone calls) to prevent	• Benefits Department • Communications Department

members from being scammed by potential imposters pretending to be ACERA staff.	
2. For terminated members with account balances, ACERA no longer receives information updates from employers. We highly recommend that if the terminated member applies to withdraw their whole ACERA account balance, it may be more secure to ask the member to provide a copy of the driver's license with their withdrawal account balance request. The copy of the driver's license can be treated as a backup to validate the withdrawal request, especially for those with a different address from ACERA's record or using a virtual-only bank, i.e., Chime. Benefit Department Comment – We are in the process of updating our term form. In addition to the need for a valid ID, requests for refund over $1,000 must be notarized unless the member presents an ID and signs in front of the team member.	• Benefits Department
3. Members changing addresses or direct deposit bank accounts, especially those using a virtual-only bank (i.e., Chime, SoFi, etc.), are higher-risk activities since recovering misappropriated funds is more challenging. We recommend that members provide a copy of their driver's license, passport, or government-issued identity card with their change request.	• Benefits Department
4. As fraud cases continue to increase, people's personal information, such as name, social security number, address, date of birth, etc., are sold on the dark web. On top of these basic four general information, we recommend the Call Center staff ask for unique personal information to authenticate members, such as years of service credit, job title, the last department worked, or the net amount of the last retirement check from ACERA. Benefits Department Comment – In July 2023, the policy was updated to include this. However, more identifiers can be added for more security.	• Benefits Department

5. The Benefits Department shall re-visit and finalize the draft “Release of Information and Member ID Policies Supplemental” document. We recommend the Call Center staff authenticate callers at the beginning of all ACERA form inquiry calls to prevent the inadvertent disclosure of member account information. (Please refer to the Test Note above.)	• Benefits Department
6. ACERA could consider looking into more advanced authentic tools, such as two-factor authentication, etc., and develop a member’s authentication smart questions library so Call Center staff can refer to those questions to authenticate callers’ identity.	• Benefits Department • PRISM • OnBase

CONTROL 2 – WEB MEMBER SERVICES (WMS) SET UP AND LOGIN

Risk Level - Medium

Control:
This control reviewed the processes of how member set up their member account in the WMS and the login process. We have asked the Benefits staff to demonstrate the WMS account setup process, what happens if the member forgets their login password, and how the user could recover/reset the password.

Risk:
The risk is that an unauthorized individual can hack into or take over the WMS account.

Audit Results:

✓ Effective

Test Notes:
For the WMS setup process, Benefits staff explained the process involved ACERA members providing / (1) the last four digits of their social security number, (2) their last name, (3) their date of birth, and (4) the home address zip code to create a new WMS account. Then, a member would create a username, password, and email for the WMS account and choose 3 of the 22 smart/personal questions for future login recovery.

For the WMS password recovery process, where a member forgot the login password, the member could answer one of the three previously designated smart/personal questions and the temporary password would be sent to the saved member email address.

However, if a member could not access their email account on record, they could contact ACERA to have an account linked to a different email account. We noted from some of the Call Center recordings that most of those members were having trouble recovering/resetting their WMS account password because they had used either their previous work email or their spouse's email when setting up their WMS account. Once they retired or divorced, they no longer had access to those email accounts to receive the password reset email sent from WMS.

We also consulted with the BASS unit about some of the technical aspects of the WMS portal. We learned that WMS was administrated and hosted by the third-party provider, LRS Retirement Solutions, which administrated Pension Gold (PG) for ACERA. The BASS unit and a few Benefit staff had a "Junior Administrator" access to the WMS portal. It allowed them to retrieve/view the member's smart/personal questions and answers. They could also help members who could not access their email reset their WMS account password. Most Benefit and Call Center staff could not view the WMS smart/personal questions.

According to BASS, LRS hosted the WMS website with its firewall. WMS did not populate directly into PG. However, there was a weekly data feed from PG to WMS for member information updates and a bi-weekly contribution transmittal file loaded to update members' account balances. A member sync wizard was being run monthly.

However, WMS allowed members to submit certain ACERA forms, which would be loaded into the OnBase documentation database.

Starting from August 2023, WMS added new security features:

1) Required password reset every 90 days;
2) New Trusted Device page – required member to answer one of the smart/personal questions if logging in from a new computer or mobile device;
3) Increased password length from up to 15 characters to up to 64 characters;
4) Only send the forgotten username to the registered email instead of appearing on screen after the member answers the smart/personal question for the forgotten username request.

Recommendations	Business Owner
1. Among calls to the Call Center regarding WMS login or password reset issues, we note that members used an email account to which they no longer had access when they originally set up their WMS account. It may be beneficial to note updating the email in the WMS portal in the new account setup process and reminding members not to use their work or spouse's email to set up their WMS account during	• Benefits Department • BASS Unit • Communication Unit • LRS

all ACERA-provided training, regular correspondence, and on the ACERA website. Benefits Department Comment - As part of the counseling process, members are directed to update their email address from the work email to a personal email address.	
2. It would be ideal if Call Center staff could access the WMS smart/personal questions without needing a WMS junior administration login so staff can use it to authenticate callers' identities.	• Benefits Department • BASS Unit • LRS

CONTROL 3 – DOCUSIGN FOR SIGNATURE SIGNING ON ACERA DOCUMENTS

Risk Level - Medium

Control:

This control reviewed how the member would use the DocuSign application to sign the ACERA forms.

Risk:

Since DocuSign was just a document signing application with no advanced security features or login requirements. It had the same exposure to the risks of forgery or fraud as the traditional paper-and-ink signatures.

Audit Results:

△ Partially Effective

Test Notes:

We discussed with Benefit staff about the process of members using the DocuSign application to provide an electronic signature for most of the ACERA forms, and some of those forms could be sent to ACERA by uploading them to the WMS portal or ACERA email address.

For many benefit requests, members needed to fill out a form, which could be done online, and the form would be sent to the designated email address provided by the requestor. Then, the requestor could use DocuSign to sign the form with an electronic signature and submit the signed form back to ACERA for review and process.

Once ACERA receives the form, Benefit staff will review and process the benefit request according to the various benefit process procedures. For signed documents using DocuSign, since we could no longer rely on matching the electronic signature to the traditional paper-and-ink signature for member authentication, the Benefits

Department established a process that benefits staff check the sender's email address to see whether it matched the member’s email address on file. If it matched, benefit staff would process the request accordingly; otherwise, staff should contact the sender for verification. This review process relied on staff self-awareness, similar to staff reviewing the traditional paper-and-ink signature.

Recommendations	Business Owner
1. DocuSign is just a signature signing application providing convenience to members. It does not have many advanced security features. Indeed, the Benefits Department has an overall verification process that validates many backup documents when a benefit request is received, including staff checking the email address where the signed form is sent for verification. However, it is sometimes difficult for a reader to tell if this particular step was performed. We recommend singling out both the signature verification for paper-and-ink signed forms and email address verification for DocuSign signed forms as a separate checkbox (or other approval method) in the procedures for all current and future OnBase workflow Processes so staff, process verifiers, and manager would be able to tell the signature has been verified.	• Benefits Department • OnBase

CONCLUSION

We audited the member authentication process and found no evidence of material weaknesses or lack of internal controls. Although there were some areas for improvement, our overall assessment is the process was deemed **PARTIALLY EFFECTIVE.**

We audited the authentication process of incoming calls to the Call Center. We also reviewed the WMS account setup, login, and signature signing on the ACERA document using the DocuSign application for any internal control weaknesses based on the current system and system security limitations.

We had made recommendations for certain areas and processes from the audit. Besides, since fraud schemes and techniques used by fraudsters are evolving and advancing constantly, we recommended that the ACERA management team meet at least once or twice a year to discuss the latest fraud trends and strengthen our process controls to resist potential fraud schemes. If necessary, we could make our annual fraud awareness training mandatory for all ACERA staff.

Benefits Department Comment –

> ACERA should consider centralizing fraud prevention, detection, and education to a focused and devoted unit. A creation of a new Fraud Prevention Unit would be responsible for member and team member education, learning new ways for ACERA to combat fraud, reviewing internal controls, systems, and processes to prevent fraud, and assisting the Benefits department in evaluating transactions to determine fraudulent activity. Fraud is not going away and will only increase in its complexity. It is our obligation to protect ACERA and our members. Unfortunately, Benefits is not able to devote the necessary resources and time to fully tackle fraud risk.

The Internal Audit Department is working with the CALAPRS to survey other California retirement systems about their member authentication processes, best practices, and what system/application they use. We aim to have the survey results for the CALAPRS Administers Roundtable Conference in December and plan to share the results with ACERA Management and the Audit Committee.

Please note that we limited this review to the areas specified in the scope section of this report. Any findings, recommendations, and conclusions outlined in this report were based on available information or otherwise obtained when this report was prepared. We thank the Benefits Department, Communications Departments, PRISM, and BASS for assisting us during the audit.