MERCED CERA
Merced County Employees' Retirement Association

AGENDA
RETIREMENT BOARD MEETING

Thursday, February 22, 2024, 8:30 A.M.

Location: Merced County Department of Public Health
260 E. 15th Street, Merced, CA 95341
Auditorium
Zoom Conference Information:
https://us06web.zoom.us/j/93030195748?pwd=NGhFeGltSVhaSTlsK2JGWE83TVFydz09
Dial In Number: 669-900-6833, MEETING ID: 930 3019 5748, PASSCODE: 095484
(For use only if Zoom Connection Malfunctions)
Telephone Number: 1-310-372-7549, Conference Code: 975839

1. **Call to Order- 8:30 A.M.**

The Retirement Board may discuss and take action on the following:

2. **Roll Call**

3. **Teleconference Request**
   Trustee Teleconference Request (Govt. Code §54953(f)(2)(A)(i)).

4. **Approval of Minutes** – January 25, 2024.

5. **Public Comment**
   Members of the public may comment on any item under the Board's jurisdiction including items on the Board's agenda. Matters presented under this item will not be discussed or acted upon by the Board at this time. Persons addressing the Board will be limited to a maximum of five (5) minutes in total. Please state your name for the record.

6. **Consent Calendar**
   Consent matters are expected to be routine and may be acted upon, without discussion, as one unit. If an item is taken off the Consent Calendar for discussion, it will be heard as the last item(s) of the Open Session as appropriate:
   a. Retirements: Pursuant to Govt. Code § 31663.25 or § 31672.

Name	Effective Date
Clanton, Paul	02/12/2024
Ellis, Angela	02/09/2024
Elms, Diane	02/05/2024
Moore, Susan	02/02/2024
Randol, Jennifer	02/02/2024

   b. Monthly Budget Report Submitted.
   c. Building Construction Budget Submitted.
   d. Meketa Monthly Performance Report Submitted.

7. **Closed Session**
   As provided in the Ralph M. Brown Act, Government Code sections 54950 et seq., the Board may meet in closed session with members of its staff, county employees and its attorneys. These sessions are not open to the public and may not be attended by members of the public. The matters the Board will meet on in closed session are identified

MERCED CERA
Merced County Employees' Retirement Association

below. Any public reports of action taken in the closed session will be made in accordance with Government Code sections 54957.1:

a. Conference with Real Property Negotiator
(Gov. Code section 54956.8.)
Property: 3199 M Street, Merced, CA
Agency negotiator: Kristen Santos
Under negotiation: Price and terms, payment or both.

8. Report Out of Closed Session

9. Open Session

a. Discussion and possible action to adopt Merced County's Cyber Security Policy – Staff.
b. Discussion and review of the newly published 2024 Capital Market Expectations by Meketa and discussion of several asset allocation options based on the Trustee Risk Survey – Meketa.
c. Discussion on the first reading of the draft Investment Beliefs Statement - Meketa.
d. Discussion and possible action to adopt a resolution honoring David Ness for his Service on the MercedCERA Board of Retirement – Staff.
e. Discussion on update of new headquarters building – Staff.

10. Information Sharing & Agenda Item Requests

11. Adjournment

The Agenda and supporting documentation, including any material that was submitted to the Merced County Employees' Retirement Association Board after the distribution of the Agenda, are available online at www.mercedcera.com.

All supporting documentation for Agenda items, including any material that was submitted to the retirement board after the distribution of the Agenda, is also available for public inspection Monday through Friday from 8:00 a.m. to 5:00 p.m. at the administrative office for the Merced County Employees' Retirement Association located at 3199 M Street, Merced, California 95348.

Persons who require accommodation for a disability in order to review an agenda, or to participate in a meeting of the Merced County Employees' Retirement Association per the American Disabilities Act (ADA), may obtain assistance by requesting such accommodation in writing addressed to Merced County Employees' Association, 3199 M Street, Merced, CA 95348 or telephonically by calling (209) 726-2724. Any such request for accommodation should be made at least 48 hours prior to the scheduled meeting for which assistance is requested.

Persons who require accommodation for any audio, visual or other disability or Spanish or Hmong interpretation in order to review an agenda, or to participate in a meeting of the Merced County Employees' Retirement Association per the American Disabilities Act (ADA), may obtain assistance by requesting such accommodation. Please address your written request to Merced County Employees' Association, 3199 M Street, Merced, CA 95348 or telephonically by calling (209) 726-2724. Any such request for accommodation should be made at least 48 hours prior to the scheduled meeting for which assistance is requested.

Spanish and Hmong interpreters are available.

Interpretes de espanol y hmong estan disponibles.
Peb muaj tug paab txhais lug Mev hab Hmoob.

MERCED CERA
Merced County Employees' Retirement Association

MINUTES
RETIREMENT BOARD MEETING

Thursday, January 25, 2024, 8:30 A.M.

Location: Merced County Department of Public Health
260 E. 15th Street, Merced, CA 95341
Auditorium
Zoom Conference Information:
https://us06web.zoom.us/j/93030195748?pwd=NGhFeGltSVhaSTlsK2JGWE83TVFydz09
Dial In Number: 669-900-6833, MEETING ID: 930 3019 5748, PASSCODE: 095484
(For use only if Zoom Connection Malfunctions)
Telephone Number: 1-310-372-7549, Conference Code: 975839

1. **Call to Order - 8:33 A.M**.

2. **Roll Call**
Board Members Present: Scott Johnston, Moses Nelson, Corrina Brown, Mike Harris, Karen Adams (left at 11:40 A.M.), Alfonse Peterson, Ryan Paskin (left at 10:28 A.M.), Janey Cabral (left at 10:28 A.M.), Aaron Rosenberg (arrived at 8:35 A.M.) ***Absent:*** Scott Silveira. ***Counsel:*** Tom Ebersole (arrived at 9:00 A.M.). ***Staff:*** Kristie Santos, Martha Sanchez Barboa, Mark Harman, Khue Xiong, Patrick Armendarez, Brenda Mojica, Monica Gallegos, Sheri Villagrana, Nikki Barraza, Kristy Barajas, and Jennifer Figueroa.

3. **Teleconference Request**
Trustee Teleconference Request (Govt. Code §54953(f)(2)(A)(i)).
Trustee Johnston requested to attend February 22, 2024 board meeting remotely due to health-related reason.
Trustee Brown requested to attend February 22, 2024 board meeting remotely due to attendance at a work-related out-of-town conference.
Board voted unanimously to approve the teleconference requests of Trustees Brown and Johnston.
1st - Adams/2nd - Peterson, passes 7/0

4. **Approval of Minutes** – December 14, 2023.
Board voted unanimously to approve the December 14, 2023 meeting minutes.
1st - Johnston/2nd - Brown, passes 7/0

5. **Public Comment**
Members of the public may comment on any item under the Board's jurisdiction including items on the Board's agenda. Matters presented under this item will not be discussed or acted upon by the Board at this time. Persons addressing the Board will be limited to a maximum of five (5) minutes in total. Please state your name for the record.
None.

6. **Consent Calendar**
Consent matters are expected to be routine and may be acted upon, without discussion, as one unit. If an item is taken off the Consent Calendar for discussion, it will be heard as the last item(s) of the Open Session as appropriate:
   a. Retirements: Pursuant to Govt. Code § 31663.25 or § 31672.

Name	Effective Date
Anaya, Yanira	12/29/2023
Battle, Regina	12/20/2023

Beeler, Shari	12/29/2023
Clark, Tracey	01/14/2024
Copus, Deborah	01/10/2024
Cortez, John	12/29/2023
De Los Reyes, Charina	01/11/2024
Gray, Elwyn	12/30/2023
Haley, Teresa	12/30/2023
Hertfelder, Dana	01/03/2024
Holder, Denise	12/30/2023
Jennings, Janet	12/14/2023
Libby, Denise	01/03/2024
Pang Her, Jean	12/30/2023
Peguero, Annette	12/30/2023
Phanith, Tim	01/13/2024
Solis, Karrie	01/08/2024
Stout, David	01/10/2024
Sullivan, Desri	12/31/2023
Storer, Bruce	12/31/2023
Swafford, Frederick (Service-Connected Disability)	09/11/2023

b. Monthly and Quarterly Budget Reports Submitted.
c. SACRS Board nomination timelines (information only).

Board voted unanimously to approve the consent agenda as presented.
1st – Cabral/2nd – Brown, passes 7/0

7. **Closed Session**

As provided in the Ralph M. Brown Act, Government Code sections 54950 et seq., the Board may meet in closed session with members of its staff, county employees and its attorneys. These sessions are not open to the public and may not be attended by members of the public. The matters the Board will meet on in closed session are identified below. Any public reports of action taken in the closed session will be made in accordance with Government Code sections 54957.1:

a. Public Employment: Chief Investment Officer (Govt. Code 54957).

8. **Report Out of Closed Session**

a. Public Employment: Chief Investment Officer (Govt. Code 54957).
Staff given direction.

9. **Open Session**

a. Discussion and possible action to adopt the proposed employer and employee contribution rates as of June 30, 2024 by MercedCERA's Actuarial Firm https://presentation.cheiron.us/presentation/view/Merced2023AVR?token=5ioc – Graham Schmidt, Cheiron.
Board voted unanimously to adopt the proposed employer and employee contribution rates as of June 30, 2024, by MercedCERA's Actuarial Firm.
1st – Adams/2nd – Peterson, passes 7/0 (Trustee Nelson voted due to Trustee Cabral leaving meeting).

b. Discussion and possible action to adopt the Cost of Living Adjustment (COLA) as recommended by Cheiron for Tier 1 members to get a COLA of at least 2.50%, with Tier 1 retirees who retired prior to April 2, 2023 receive an increase of 3.00%, due to their carry-over balances as of April 1, 2023, with the remaining

carry-over balances reduced by 0.5% (the amount of the COLA increase in excess of 2.50%) – Graham Schmidt, Cheiron.
Board voted unanimously to adopt the Cost of Living Adjustment (COLA) as recommended by Cheiron for Tier 1 members to get a COLA of at least 2.50%, with Tier 1 retirees who retired prior to April 2, 2023 receive an increase of 3.00%, due to their carry-over balances as of April 1, 2023, with the remaining carry-over balances reduced by 0.5% (the amount of the COLA increase in excess of 2.50%)
1st – Brown/2nd – Peterson, passes 7/0

c. Discussion and possible action to adopt the audit report for MercedCERA and adopt the Annual Comprehensive Financial Report (ACFR) – UHY.
Board voted to adopt the Annual Audit Report for MercedCERA and adopt the Annual Comprehensive Financial Report (ACFR).
1st – Adams/2nd – Brown, passes 7/0

d. Discussion and possible action or direction on Meketa's monthly performance report, education timeline and investment survey discussion – Meketa Group.
No action taken.

e. Chair to appoint budget ad hoc subcommittee to work with staff on FY 2024/2025 budget – Chair.
Agenda item postponed for future meeting.

f. Discussion on update of new headquarters building – Staff.
Agenda Item postponed for future meeting.

10. <u>Information Sharing & Agenda Item Requests</u>
Kristie informed that the MercedCERA Board Meeting space would be in this same location through May.
Merced County Department of Public Health, 260 E. 15th Street, Merced, CA 95341, Auditorium

11. <u>Adjourned</u> - 11:48 .A.M.

Accepted By,

Trustee Name/Position	Signature	Date
Ryan Paskin/Chair		
Al Peterson/Secretary		

Merced County Employees' Retirement Association
Non-Administrative Expenditures Report (Preliminary)
For the Month Ended January 31, 2024

Non-Administrative Expenses	Original Projection	Current Projection	Expended 2024-01	Expended YTD	Bal Remaining	% Exp YTD
21800 · Investment Expenses	**3,740,500.00**	**3,740,500.00**	**175,407.66**	**1,258,086.60**	**2,482,413.40**	**34%**
1/5/2024 Office Payroll 2024 PP 01 - Staff Investment Allocation			18,115.46			
1/9/2024 Meketa - Oct-Dec 2023 Consulting Svcs			54,133.50			
1/11/2024 Taconic MDOF III - 2023-Q3 & Q4 Mgt Fees			43,163.52			
1/17/2024 Driehaus - 2023-Q4 Mgt Fees			28,174.00			
1/19/2024 Office Payroll 2024 PP 02 - Staff Investment Allocation			17,539.59			
1/25/2024 Mellon LC SIF - 2023-Q4 Mgt Fees			14,281.59			
Total 21800 · Investment Expenses			**175,407.66**			
21802 · Actuarial Services	**175,000.00**	**175,000.00**	**37,268.00**	**67,888.00**	**107,112.00**	**39%**
1/18/2024 Cheiron - 2023-Q4 Actuarial Svcs			44,302.50			
1/18/2024 Reimb from County for GASB 67/68 Actuarial Costs			(6,577.32)			
1/31/2024 Reimb from Court for Gasb 68 Actuarial Costs			(457.18)			
Total 21802 · Actuarial Services			**37,268.00**			
21812 · Data Processing	**102,000.00**	**102,000.00**	**8,771.58**	**44,790.78**	**57,209.22**	**44%**
1/23/2024 2023-12 Cradlepoint Chgs			703.00			
1/23/2024 2023-12 IS Billing			7,762.23			
1/23/2024 Comcast - Feb 2024 Svcs			306.35			
Total 21812 · Data Processing			**8,771.58**			
21834 · Legal Services	**430,000.00**	**430,000.00**	**13,703.16**	**161,900.69**	**268,099.31**	**38%**
1/5/2024 2024-10 Cost Alloc - Co Couns			5,632.50			
1/5/2024 Ted Cabral - 2023-12 Legal Svcs			2,123.60			
1/5/2024 Ted Cabral - 2023-12 Legal Svcs			49.56			
1/5/2024 Ted Cabral - 2023-12 Legal Svcs			100.00			
1/5/2024 Ted Cabral - 2023-12 Legal Svcs			1,524.80			
1/5/2024 Ted Cabral - 2023-12 Legal Svcs			1,739.00			
1/23/2024 Hanson Bridgett - 2023-12 Legal Svcs			2,087.10			
1/29/2024 Nossman - 2023-12 Gen Adv & Counsel			446.60			
Total 21834 · Legal Services			**13,703.16**			
21840 · Custodial Banking Services	**150,000.00**	**150,000.00**	**1,259.74**	**41,460.41**	**108,539.59**	**28%**
1/2/2024 2023-11 Wire Fees			165.00			
1/4/2024 2023-12 NT STIF Income - Cust Fee			1,094.74			
Total 21840 · Custodial Banking Services			**1,259.74**			

Merced County Employees' Retirement Association
Non-Administrative Expenditures Report (Preliminary)
For the Month Ended January 31, 2024

Non-Administrative Expenses		Original Projection	Current Projection	Expended 2024-01	Expended YTD	Bal Remaining	% Exp YTD
22350 · Software and Technology		**505,000.00**	**505,000.00**	**6,681.38**	**312,440.96**	**192,559.04**	**62%**
1/2/2024	Pitney Bowes - Postal Meter Quarterly Charges			210.96			
1/2/2024	LexisNexis - 2023-11 Accurint & Batch Svcs			599.71			
1/5/2024	PensionX - 2024-01 Svc Program & SLA			900.00			
1/5/2024	GFOA - Membership Renewal Thru 2024-11			570.00			
1/18/2024	Spriggs - 2024-Q1 Contract Base Rate			1,288.95			
1/23/2024	LexisNexis - 2023-12 Accurint & Batch Svcs			599.16			
1/23/2024	Spriggs - 2023-Q4 Contract Usage Charge			221.29			
1/24/2024	Reimb employee for Monitors, Cable, Headset			176.00			
1/24/2024	ODP Business Solutons - VersaDesk			466.01			
1/29/2024	Zoom Video Comm - Annual Subscription			1,649.30			
Total 22350 · Software and Technology				**6,681.38**			
Depreciation Expense		**250,000.00**	**250,000.00**	**-**	**-**	**250,000.00**	
Total Non-Administrative Items		**5,352,500.00**	**5,352,500.00**	**243,091.52**	**1,886,567.44**	**3,465,932.56**	**35%**

Merced County Employees' Retirement Association
Non-Administrative Expenses Prev Year Comparison (Preliminary)
01/31/2024

	January 2024	January 2023	$ Change	% Change
Expense				
62025 · Non-Administrative Expenses				
21800 · Investment Expenses	$ 175,407.66	$ 139,306.61	$ 36,101.05	25.92%
21802 · Actuarial Services	37,268.00	-	$ 37,268.00	100.00%
21812 · Data Processing	8,771.58	5,067.70	3,703.88	73.09%
21834 · Legal Services	13,703.16	14,823.05	(1,119.89)	-7.56%
21840 · Custodial Banking Services	1,259.74	26,045.10	(24,785.36)	-95.16%
22350 · Software and Technology	6,681.38	2,961.06	3,720.32	125.64%
Depreciation Expense	-	-	-	
Total 62025 · Non-Administrative Expenses	$ 243,091.52	$ 188,203.52	$ 54,888.00	29.16%

Merced County Employees' Retirement Association
Administrative Expenditures Report (Preliminary)
For the Month Ended January 31, 2024

Administrative Budget	Adopted	Current Budget	Expended 2024-01	Expended YTD	Bal Remaining	% Exp YTD
10110 · Salaries & Wages	**1,975,000.00**	**1,975,000.00**	**107,785.36**	**683,564.66**	**1,291,435.34**	**35%**
1/5/2024 Office Payroll 2024 PP 01 - Administrative Allocation			53,988.56			
1/19/2024 Office Payroll 2024 PP 02 - Administrative Allocation			53,796.80			
Total 10110 · Salaries & Wages			**107,785.36**			
20600 · Communications	**9,800.00**	**9,800.00**	**919.92**	**4,685.84**	**5,114.16**	**48%**
1/2/2024 AT&T - 2023-12 CALNET			165.46			
1/23/2024 2023-12 Comm Chgs			325.45			
1/23/2024 2023-12 Cell Chgs			263.00			
1/31/2024 AT&T - 2024-01 CALNET			166.01			
Total 20600 · Communications			**919.92**			
20900 · Household Expense	**15,750.00**	**15,750.00**	**1,112.56**	**7,593.24**	**8,156.76**	**48%**
1/9/2024 Bob's Pest Control - 2023-12 Pest Control			40.00			
1/16/2024 Geil Enterprises - 2024-01 Janitorial Svcs			959.00			
1/17/2024 ADT - Jan 2024 Security Svcs			56.78			
1/17/2024 ADT - Feb 2024 Security Svcs			56.78			
Total 20900 · Household Expense			**1,112.56**			
21000 · Insurance - Other	**105,000.00**	**105,000.00**	**-**	**101,995.00**	**3,005.00**	**97%**
Total 21000 · Insurance - Other			**-**			
21301 · Maintenance Structure Improvement	**16,000.00**	**16,000.00**	**460.00**	**5,463.91**	**10,536.09**	**34%**
1/9/2024 Yard Masters - 2024-01 Shrub Pruning			100.00			
1/24/2024 Yard Masters - 2024-01 Landscape Svcs			360.00			
Total 21301 · Maintenance Structure Improvement			**460.00**			
21500 · Membership	**8,000.00**	**8,000.00**		**5,805.00**	**2,195.00**	**73%**
Total 21500 · Membership			**-**			
21700 · Office Expense - General	**19,275.00**	**19,275.00**	**997.45**	**12,230.88**	**7,044.12**	**63%**
1/9/2024 First Choice - 2024-01 Water Svcs			116.55			
1/23/2024 First Choice - 2024-01 Water Svcs - 2nd Delivery			97.91			
1/23/2024 2024-01 Stores Billing			782.99			
Total 21700 · Office Expense - General			**997.45**			
21710 · Office Expense - Postage	**20,000.00**	**20,000.00**	**1,862.05**	**11,288.61**	**8,711.39**	**56%**
1/23/2024 2023-12 Mailroom Chgs			1,862.05			
Total 21710 · Office Expense - Postage			**1,862.05**			
21805 · Audits	**65,000.00**	**65,000.00**	**49,610.00**	**49,610.00**	**15,390.00**	**76%**
1/2/2024 GFOA - Cert of Achiev Fee FY 2023			610.00			
1/9/2024 UHY - 2023 Audit Progress Thru 12/5/2023			39,000.00			
1/17/2024 UHY - 2023 GASB 68 Audit			6,000.00			
1/17/2024 UHY - 2023 Audit Progress Final Billing			7,000.00			
1/18/2024 Reimb from County for GASB 67/68 Audit Costs			(2,805.03)			
1/31/2024 Reimb from Courts for GASB 68 Audit Costs			(194.97)			
Total 21805 · Audits			**49,610.00**			

Merced County Employees' Retirement Association
Administrative Expenditures Report (Preliminary)
For the Month Ended January 31, 2024

Administrative Budget	Adopted	Current Budget	Expended 2024-01	Expended YTD	Bal Remaining	% Exp YTD
21808 · Board Membership	**10,000.00**	**10,000.00**	**322.95**	**3,622.95**	**6,377.05**	**36%**
1/31/2024 2024-01 Board Mtg Expense			322.95			
Total 21808 · Board Membership			**322.95**			
21900 · Publications & Legal Notices	**5,000.00**	**5,000.00**	**-**	**3,759.57**	**1,240.43**	**75%**
Total 21900 · Publications & Legal Notices			**-**			
22300 · Spec Dept Exp - Other	**750.00**	**750.00**	**-**	**38.99**	**711.01**	**5%**
Total 22300 · Spec Dept Exp - Other			**-**			
22310 · Election Expense	**30,000.00**	**30,000.00**	**-**	**5,541.41**	**24,458.59**	**18%**
Total 22310 · Election Expense			**-**			
22327 · Spec Dept Exp - Cost Allocation	**40,000.00**	**40,000.00**	**3,298.50**	**23,089.50**	**16,910.50**	**58%**
1/5/2024 2024-01 Cost Alloc			3,298.50			
Total 22327 · Spec Dept Exp - Cost Allocation			**3,298.50**			
22500 · Transportation & Travel	**250.00**	**250.00**	**-**	**52.86**	**197.14**	**21%**
Total 22500 · Transportation & Travel			**-**			
22505 · Trans & Travel - Staff Development	**4,000.00**	**4,000.00**		**149.00**	**3,851.00**	**4%**
Total 22505 · Trans & Travel - Staff Development			**-**			
22515 · Trans & Travel - In State	**40,000.00**	**40,000.00**	**100.00**	**14,014.00**	**25,986.00**	**35%**
1/23/2024 CALAPRS - 2024-02 Administrators RT Reg Fee			50.00			
1/24/2024 Reimb for CALAPRS - 2024-02 Administrators RT Reg Fee			50.00			
Total 22515 · Trans & Travel - In State			**100.00**			
22516 · Trans & Travel - Out of State	**7,500.00**	**7,500.00**	**-**	**3,481.31**	**4,018.69**	**46%**
Total 22516 · Trans & Travel - Out of State			**-**			
22600 · Utilities	**20,000.00**	**20,000.00**	**2,699.87**	**11,500.73**	**8,499.27**	**58%**
1/3/2024 PG&E - Dec 2023 Svcs			1,072.00			
1/16/2024 City of Merced - Jan 2024 WS&G			245.33			
1/31/2024 PG&E - Jan 2024 Svcs			1,382.54			
Total 22600 · Utilities			**2,699.87**			
Depreciation Expense	**27,000.00**	**27,000.00**	**-**	**-**	**27,000.00**	
Total Administrative Budget	**2,418,325.00**	**2,418,325.00**	**169,168.66**	**947,487.46**	**1,470,837.54**	**39%**

Merced County Employees' Retirement Association
New Headquarters Expenditure Report
Through the Month Ended January 31, 2024

MercedCERA New Headquarters Expenditures

Land and Due Diligence Expenditures

08/01/2019	Golden Valley Engineering - Inv 106670 - 2019-07 Due Diligence New Building	3,225.00
08/12/2019	Golden Valley Engineering - Inv 106727 - 2019-07 Due Diligence New Building	11,877.50
10/03/2019	Nossaman - Inv 500498 - 2019-08 - Real Estate Purchase Related Legal	3,707.55
10/10/2019	Golden Valley Engineering - Inv 106900 - 2019-09 Due Diligence New Building	3,277.50
10/23/2019	**TransCounty Title - Purchase of Land for New MCERA Building**	**352,585.00**
11/05/2019	Golden Valley Engineering - Inv 106900 - 2019-10 Due Diligence - New Building	9,357.25
11/05/2019	Nossaman - Inv 501678 - 2019-09 - Real Estate Purchase Related Legal	3,288.60
12/05/2019	Nossaman - Inv 502566 - 2019-10 - Real Estate Purchase Related Legal	5,481.91
01/30/2020	Golden Valley Engineering - Inv107252 - Thru 2020-01-11 Due Diligence - New Building	4,492.50
01/30/2020	Nossaman - Inv 503888 - 2019-11 - Real Estate Purchase Related Legal	2,506.67
01/30/2020	Nossaman - Inv 504751 - 2019-12 - Real Estate Purchase Related Legal	1,289.25
01/31/2020	Golden Valley Engineering - Inv107210 - Thru 2019-12-28 Due Diligence - New Building	4,572.50
02/07/2020	Golden Valley Engineering - Inv107301 - Thru 2020-01-25 Due Diligence - New Building	432.50
02/24/2020	Golden Valley Engineering - Inv107349 - Thru 2020-02-08 Due Diligence - New Building	1,140.00
03/10/2020	Golden Valley Engineering - Inv107387 - Thru 2020-02-22 Due Diligence - New Building	1,165.00
04/09/2020	Golden Valley Engineering - Inv107451 - Thru 2020-03-21 Due Diligence - New Building	2,132.50
06/29/2020	Golden Valley Engineering - Inv107881 - 2020-03-21 Thru 2020-06-21 Due Diligence - New Building	523.13
06/29/2020	Nossaman - Inv 505773 - 2020-01-Potential Real Estate Purchase by MCERA	987.45
08/21/2020	Golden Valley Engineering - Inv107881 - Thru 2020-07-25 Due Diligence - New Building	174.37
09/22/2020	Nossaman - Inv 513318 - 2020-08 - MCERA New Building	144.45
03/16/2021	Golden Valley Engineering - Inv 108508 - Thru 2021-02-20 Due Diligence - New Building	120.00
06/02/2021	Golden Valley Engineering - Inv 108836 - Thru 2021-05-15 Due Diligence - New Building	240.00
11/03/2021	Golden Valley Engineering - Inv 109356 - New Building Due Diligence thru 2021-10-16	180.00
11/10/2021	Golden Valley Engineering - Inv 109429 - New Bldg Due Diligence Thru 10/31/2021	1,928.00
03/01/2022	Nossaman - Inv 531558 - 2022-01 New Bldg Legal	2,740.05
06/08/2022	Nossaman - Inv 535102 - 2022-04 New Bldg	155.25
Total Land & Due Diligence Expenditures		**417,723.93**

Maintenance Expenditures

12/04/2019	J & B Fencing - Inv 943 - 2019-11 Temp Fencing Installment	1,980.00
02/11/2020	Yard Masters - Inv16037 - 2020-01 - New Building Weed Abatement	250.00
06/29/2020	Yard Masters - Inv16825 - 2020-06 - New Building Weed Abatement	300.00
02/01/2021	J & B Fencing - Inv 1027 - 2 Months of Temp Fencing Rental	300.00
04/19/2021	J & B Fencing - Inv 1156 - 3 Months of Temp Fencing Rental (Feb, Mar, Apr)	450.00
11/03/2021	J & B Fencing - Inv 1329 - 2021-05 - 2021-11 Fencing at 19th & N.	1,050.00
03/17/2022	Yard Masters - Inv 20451 - Weed Control for New Bldg	950.00
06/20/2022	J & B Fencing - Inv 1453 - 2021-12 thru 2022-05 Fence Rental	900.00
08/16/2022	J & B Fencing - Inv 1472 - 2022-06 thru 2022-08 Fence Rental	450.00
09/21/2022	J & B Fencing - Inv 1501 - 2022-09 Fence Rental	350.00
12/09/2022	J&B Fencing - Inv 1548 - 2022-10 Thru 2022-12 Fence Rental	1,050.00
02/27/2023	J&B Fencing - Inv 1582 - 2023-01 Thru 2023-02 Fence Rental	700.00
04/28/2023	Yard Masters - Inv 23021 - Weed Abatement at New Building Lot	975.00
06/29/2023	J&B Fencing - Inv 1640 - 2023-03 thru 2023-06 Fencing	1,400.00
11/21/2023	J&B Fencing - Inv 1681 - 2023-07 thru 2023-09 Fencing	1,050.00
Total Maintenance Expenditures		**12,155.00**

Merced County Employees' Retirement Association
New Headquarters Expenditure Report
Through the Month Ended January 31, 2024

Architectural, Engineering, and Construction Expenditures (Budgeted per Hilbers Contract)		
06/29/2022	Golden Valley Engineering - Inv 110079 - Prof Svcs thru 2022-06-20	18,862.50
06/29/2022	Golden Valley Engineering - Inv 110118 - Prof Svcs thru 2022-06-25	10,620.00
09/08/2022	Golden Valley Engineering - Inv 1101022 - Prof Svcs thru 2022-08-20	16,747.50
09/20/2022	Golden Valley Engineering - Inv 1100934 - Prof Svcs thru 2022-07-23	11,850.00
09/20/2022	Golden Valley Engineering - Inv 110157 - Prof Svcs thru 2022-07-09	7,007.50
09/21/2022	Golden Valley Engineering - Inv 1101056 - Prof Svcs thru 2022-09-03	6,672.50
10/07/2022	Golden Valley Engineering - Inv 1101130 - Prof Svcs thru 2022-10-01	10,577.50
10/31/2022	Golden Valley Engineering - Inv 1101081 - Prof Svcs thru 2022-09-17	10,480.00
10/31/2022	Golden Valley Engineering - Inv 1101217 - Prof Svcs thru 2022-10-15	16,850.50
11/08/2022	Golden Valley Engineering - Inv 1101255 - Prof Svcs thru 2022-10-29	12,092.50
11/23/2022	Golden Valley Engineering - Inv 1101329 - Prof Svcs thru 2022-11-12	19,325.00
12/06/2022	Golden Valley Engineering - Inv 1101374 - Prof Svcs thru 2022-11-26	14,042.50
12/29/2022	Golden Valley Engineering - Inv 1101434 - Prof Svcs thru 2022-12-23	27,410.50
02/01/2023	Golden Valley Engineering - Inv 1101432 - Prof Svcs thru 2022-12-10	26,499.50
02/01/2023	Golden Valley Engineering - Inv 1101533 - Prof Svcs thru 2023-01-21	6,560.00
02/14/2023	Golden Valley Engineering - Inv 1101548 - Prof Svcs thru 2023-02-04	3,030.00
03/07/2023	Golden Valley Engineering - Inv 1101659 - Prof Svcs thru 2023-02-18	9,040.00
03/17/2023	Golden Valley Engineering - Inv 1101675 - Prof Svcs thru 2023-03-04	14,260.00
03/31/2023	Golden Valley Engineering - Inv 1101749 - Prof Svcs thru 2023-03-18	6,820.00
04/28/2023	Golden Valley Engineering - Inv 1101839 - Prof Svcs thru 2023-04-15	7,047.50
05/25/2023	Golden Valley Engineering - Inv 1101893 - Prof Svcs Thru 2023-04-29	1,255.00
06/16/2023	Golden Valley Engineering - Inv 1101975 - Prof Svcs thru 2023-05-27	8,109.50
06/29/2023	Golden Valley Engineering - Svcs Thru 2023-06-10	5,602.00
08/01/2023	Golden Valley Engineering - Inv 1102166 - Prof Svcs Thru 2023-07-08	260.00
08/17/2023	Golden Valley Engineering - Inv 1102232 - Prof Svcs Thru 2023-07-22	7,552.50
10/02/2023	Golden Valley Engineering - Inv 1102416 - 2023-07 thru 2023-09	13,111.25
11/22/2023	Hilbers Inc - New HQ Bldg Progress Pymt 1	195,024.68
11/27/2023	Hilbers Inc - Inv 23-1132 - Permit & Process Fee - New Bldg	38,411.16
11/28/2023	Golden Valley Engineering - Inv 1102541 - Prof Svcs Thru 2023-10-28	8,867.50
11/28/2023	Golden Valley Engineering - Inv 1102606 - Prof Svcs Thru 2023-11-11	7,860.00
12/14/2023	Golden Valley Engineering - Inv 1102656 Prof Svcs Thru 2023-11-25	15,369.50
12/21/2023	RMA Geoscience Inc - Inv 17540 - Prof Svcs 2023 Oct 16-Nov 12	1,443.25
12/27/2023	Golden Valley Engineering - Inv 1102689 - Prof Svcs Thru 2023-12-09	2,310.00
12/28/2023	Hilbers Inc - New HQ Bldg Progress Pymt 2	370,256.66
01/18/2024	Golden Valley Engineering - Inv 1102729 - Prof Svcs Thru 2024-01-06	20,679.58
01/22/2024	RMA Geoscience Inc - Inv 17732 - Prof Svcs 2023-11-13 thru 2023-12-10	8,242.25
Total Architectural, Engineering, and Construction Expenditures		**960,150.33**
Total Budgeted for Architectural, Engineering, & Construction		**10,591,802.40**
Balance Remaining		**9,631,652.07**
Percentage Expended		**9.07%**
All new headquarters building-related expenditures through 01/31/2024		**1,390,029.26**

MEKETA

Merced County Employees' Retirement Association

February 22, 2024

Q4 Performance Update

Table of Contents

Economic and Market Update

Data as of December 31, 2023

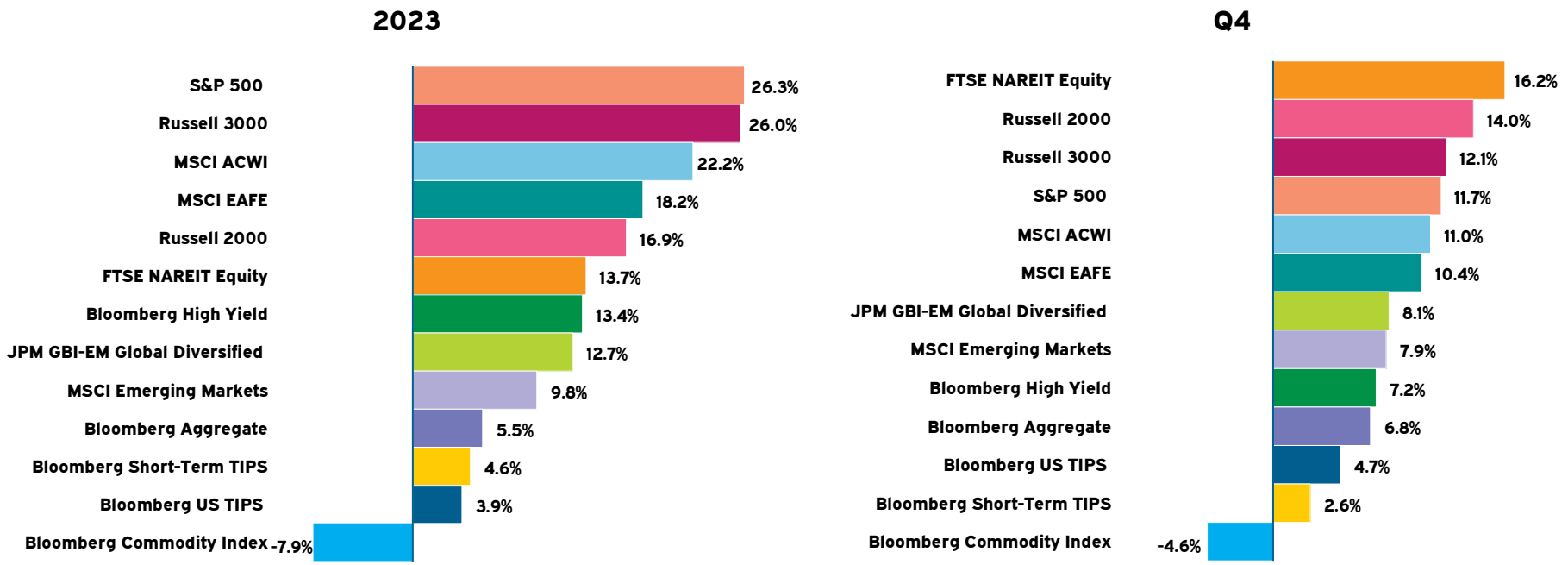
Commentary

→ Most markets rallied in the fourth quarter in anticipation that policy rates cuts were ahead in 2024.

- Major central banks have largely paused interest rates hikes. Markets are now largely expecting the FOMC to maintain interest rates at the current levels and begin cutting rates as soon as Q1 2024.
- Inflation rose in December in the US and Europe, but both finished the year much lower than where they started. China remained in deflationary territory (-0.3%) at year-end.
- US equity markets (Russell 3000 index) posted strong gains for the quarter (12.1%), raising full year results to +26.0%. Most sectors rallied, with more defensive sectors lagging.
- Non-US developed equity markets also rallied in the fourth quarter (MSCI EAFE 10.4%), with the weakening of the US dollar contributing meaningfully (10.4% versus 5.0% ex.-US dollar influence). The performance difference between US and international developed equities for the year remained wide (26.0% versus 18.2%).
- Emerging market equities were up 7.9% in the fourth quarter and 9.8% for calendar 2023 but trailed developed markets due to lagging returns in China (-4.2% Q4/-11.2% one-year). Emerging market equities ex.-China returned 20% in 2023.
- Interest rates generally fell in the fourth quarter, particularly for longer-dated maturities. The broad US bond market rallied (6.8%) for the quarter, lifting 2023 returns into positive territory (5.5%).

→ Looking to 2024, the paths of inflation and monetary policy, China's economic disorder and slowing economic growth, and the wars in Ukraine and Israel, will be key.

Index Returns[1]



→ After a tough start to the quarter on lingering fears that the Federal Reserve might keep interest rates "higher for longer", markets rallied in November and December. Economic data generally coming in below expectations sparked expectations that the Federal Reserve might really be done raising policy rates for this cycle.

→ Strong results for the quarter built on gains for the year with all asset classes finishing in positive territory in 2023, except commodities.

[1] Source: Bloomberg. Data is as of December 31, 2023.

Domestic Equity Returns[1]

Domestic Equity	December (%)	Q4 (%)	1 YR (%)	3 YR (%)	5 YR (%)	10 YR (%)
S&P 500	4.5	11.7	26.3	10.0	15.7	12.0
Russell 3000	5.3	12.1	26.0	8.6	15.2	11.5
Russell 1000	4.9	12.0	26.5	9.0	15.5	11.8
Russell 1000 Growth	4.4	14.2	42.7	8.9	19.5	14.9
Russell 1000 Value	5.5	9.5	11.5	8.9	10.9	8.4
Russell MidCap	7.7	12.8	17.2	5.9	12.7	9.4
Russell MidCap Growth	7.6	14.5	25.9	1.3	13.8	10.6
Russell MidCap Value	7.8	12.1	12.7	8.4	11.2	8.3
Russell 2000	12.2	14.0	16.9	2.2	10.0	7.2
Russell 2000 Growth	12.0	12.7	18.7	-3.5	9.2	7.2
Russell 2000 Value	12.4	15.3	14.6	8.0	10.0	6.8

US Equities: The Russell 3000 rallied 5.3% in December, bringing fourth quarter results to +12.1%. US stocks were up 26.0% in 2023.

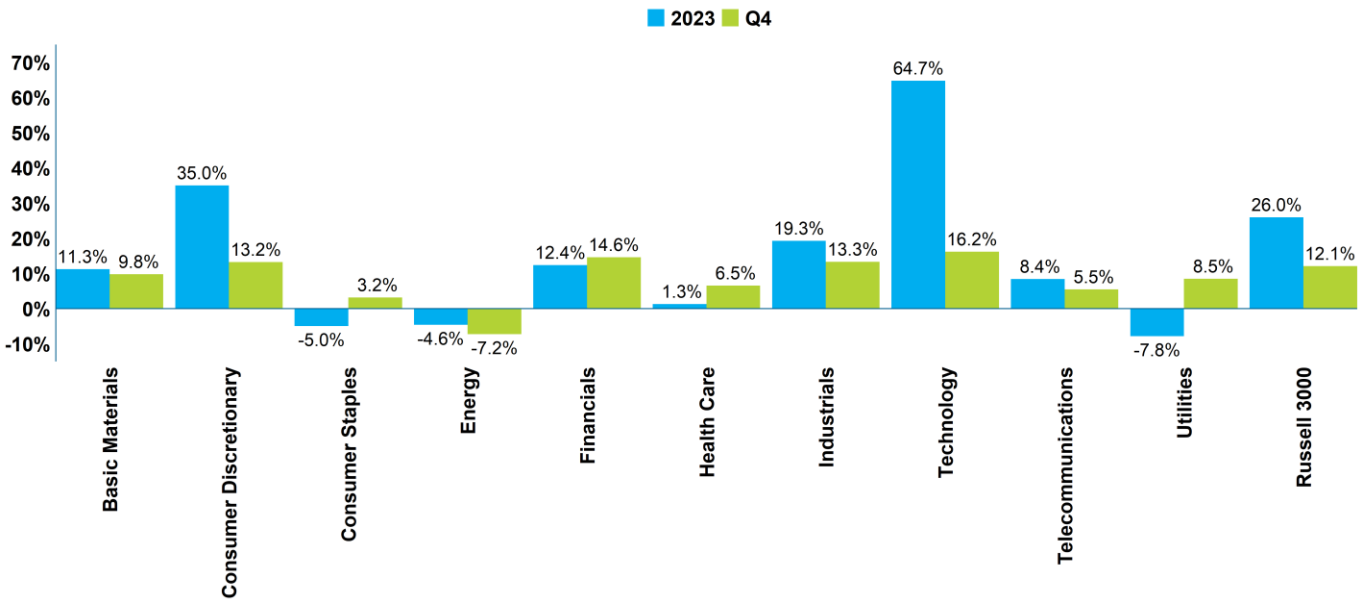
→ US equities had a strong final quarter of the year, driven by expectations that rate cuts may be ahead in 2024.

→ Small cap stocks outperformed their large cap peers for the quarter while growth outpaced value with the exception of small cap. Large cap stocks outperformed small cap stocks by a wide margin for the calendar year and growth outpaced value across market caps.

→ Calendar year results were clearly driven by large cap technology stocks. Within the S&P 500 index, the "Magnificent 7" stocks generated more than 50% of the total gains.

[1] Source: Bloomberg. Data is as of December 31, 2023. Magnificent Seven stocks include: Apple, Microsoft, Alphabet, Amazon, Nvidia, Tesla, and Meta.

Russell 3000 Sector Returns[1]



→ All sectors posted gains for the fourth quarter, except for energy (-7.2%) given oil's recent declines. Technology (+16.2%) led the way for the quarter followed by financials (+14.6%).

→ In 2023, technology (+64.7%) and consumer discretionary (+35.0%) sectors had the best results, helped respectively by artificial intelligence optimism and a healthy US consumer. Traditionally defensive sectors like utilities (-7.8%) and consumer staples (-5.0%) trailed.

[1] Source: Bloomberg. Data is as of December 31, 2023.

Foreign Equity Returns[1]

Foreign Equity	December (%)	Q4 (%)	1 YR (%)	3 YR (%)	5 YR (%)	10 YR (%)
MSCI ACWI ex. US	5.0	9.8	15.6	1.5	7.1	3.8
MSCI EAFE	5.3	10.4	18.2	4.0	8.2	4.3
MSCI EAFE (Local Currency)	2.9	5.0	16.2	8.7	9.5	6.6
MSCI EAFE Small Cap	7.3	11.1	13.2	-0.7	6.6	4.8
MSCI Emerging Markets	3.9	7.9	9.8	-5.1	3.7	2.7
MSCI Emerging Markets (Local Currency)	3.1	5.6	9.9	-2.5	5.4	5.2
MSCI China	-2.4	-4.2	-11.2	-18.5	-2.8	0.9

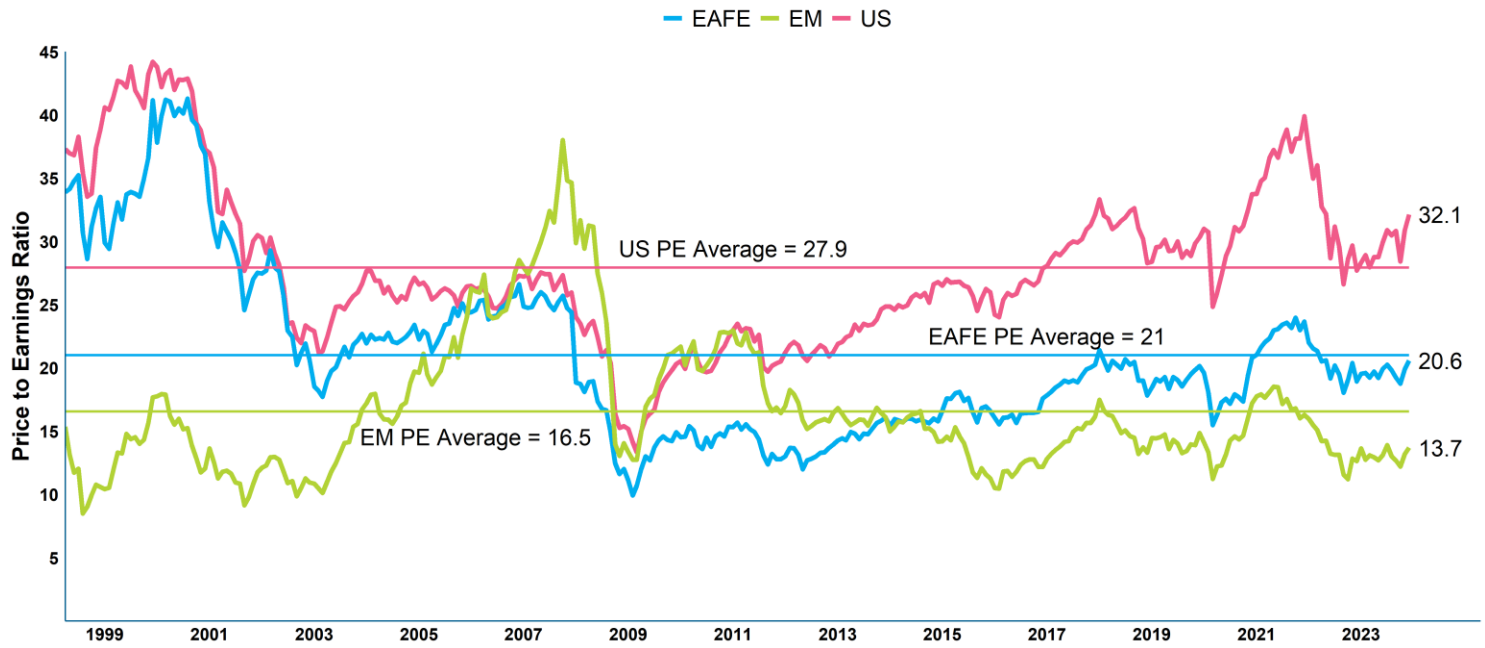
Foreign Equity: Developed international equities (MSCI EAFE) gained 5.3% in December and 10.4% in the fourth quarter bringing calendar year results to 18.2%. Emerging market equities (MSCI EM) rose 3.9% in December, 7.9% for the quarter, and 9.8% for the year.

→ Optimism around lower inflation and potentially peaking and declining policy rates drove gains in the UK and Europe. Japan had weaker results for the quarter as concerns over a strengthening yen weighed on returns in December. Overall weakness in the US dollar also contributed to quarterly and full year results across developed markets.

→ Emerging markets also experienced strong performance in the fourth quarter but trailed developed markets. China weighed on relative results for the quarter and year, declining 4.2% and 11.2%, respectively. Slowing growth, issues in the property sector, and on-going tensions with the US all weighed on results.

[1] Source: Bloomberg. Data is as of December 31, 2023.

Equity Cyclically Adjusted P/E Ratios[1]



→ Given the strong technology-driven rally last year, the US equity price-to-earnings ratio increased above its 21st century average. Fourth quarter gains brought valuations to their highest level for the year.

→ International market valuations also increased in the fourth quarter, but remain below the US. In the case of developed markets, valuations finished the year close to the their long-term average, while emerging markets remained well below their average.

[1] US Equity Cyclically Adjusted P/E on S&P 500 Index. Source: Robert Shiller, Yale University, and Meketa Investment Group. Developed and Emerging Market Equity (MSCI EAFE and EM Index) Cyclically Adjusted P/E – Source: Bloomberg. Earnings figures represent the average of monthly "as reported" earnings over the previous ten years. Data is as of December 2023. The average line is the long-term average of the US, EM, and EAFE PE values from April 1998 to the recent month-end respectively.

Fixed Income Returns[1]

Fixed Income	December (%)	Q4 (%)	1 YR (%)	3 YR (%)	5 YR (%)	10 YR (%)	Current Yield (%)	Duration (Years)
Bloomberg Universal	3.8	6.8	6.2	-3.0	1.4	2.1	4.8	6.1
Bloomberg Aggregate	3.8	6.8	5.5	-3.3	1.1	1.8	4.5	6.3
Bloomberg US TIPS	2.7	4.7	3.9	-1.0	3.2	2.4	4.2	6.7
Bloomberg Short-term TIPS	1.1	2.6	4.6	2.3	3.4	2.0	4.5	2.4
Bloomberg High Yield	3.7	7.2	13.4	2.0	5.4	4.6	7.6	3.8
JPM GBI-EM Global Diversified (USD)	3.2	8.1	12.7	-3.2	1.1	0.1	6.5	5.0

Fixed Income: The Bloomberg Universal index rose 3.8% in December, 6.8% for the quarter, and 6.2% for the year.

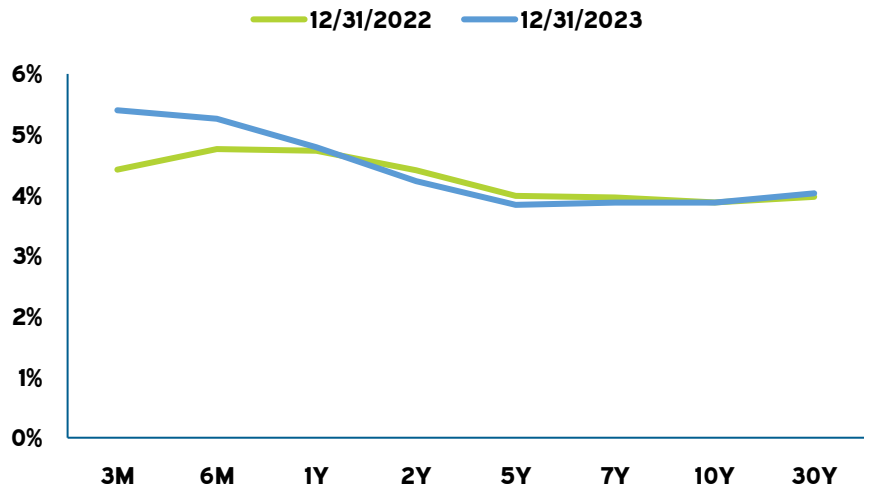
→ Policy rate expectations swung from pessimism to optimism in November and December. Signs of the labor market cooling and improving inflation led investors to bring forward expectations for interest rate cuts to early 2024, leading to one of the best quarterly results in over twenty years.

→ The broad US bond market (Bloomberg Aggregate) rallied 6.8% for the quarter, lifting full-year performance into positive territory (+5.5%). The broader TIPS index rose 4.7% for the quarter and 3.9% for the year, while the less interest-rate-sensitive short-term TIPS index rose 2.6% and 4.6% over the same periods.

→ High yield bonds rallied on better risk sentiment (+7.2%), as did emerging market bonds (+8.1%). Both asset classes produced double-digit results last year.

[1] Source: Bloomberg. JPM GBI-EM data is from InvestorForce. Data is as of December 31, 2023. The yield and duration data from Bloomberg is defined as the index's yield to worst and modified duration respectively.

US Yield Curve[1]



→ The more policy sensitive short-term maturities were higher this year while longer-term maturities finished the year where they started.

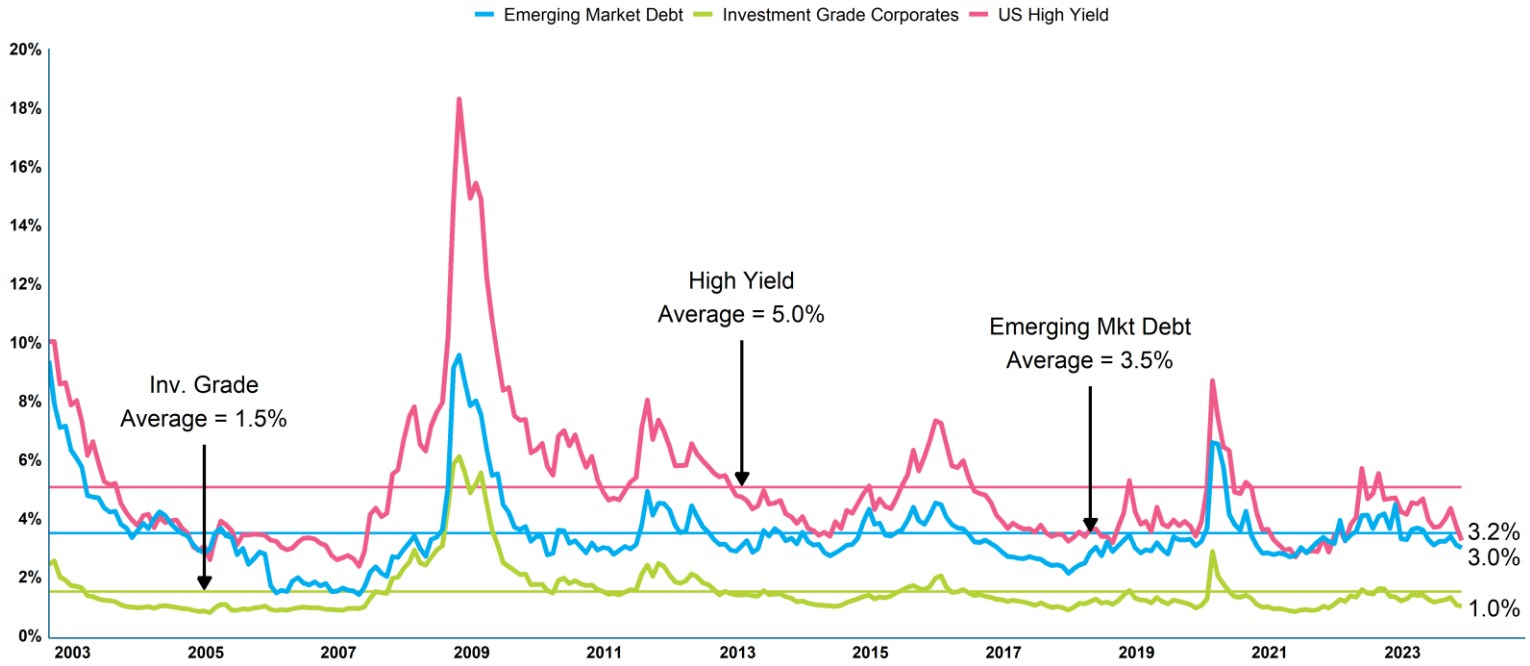
→ Still, rates declined sharply over the quarter, particularly at the longer end of the yield curve on continued easing of inflation-related risks and speculation that the Federal Reserve is done with their policy rate increases for this cycle.

→ For the quarter, two-year Treasury yields fell from 5.05% to 4.24% while ten-year Treasury yields declined from 4.56% to 3.88%.

→ The yield curve remained inverted at year-end despite a recent flattening trend. The spread between the 2-year and 10-year Treasury was -0.37% at the end of December.

[1] Source: Bloomberg. Data is as of December 31, 2023.

Credit Spreads vs. US Treasury Bonds[1]

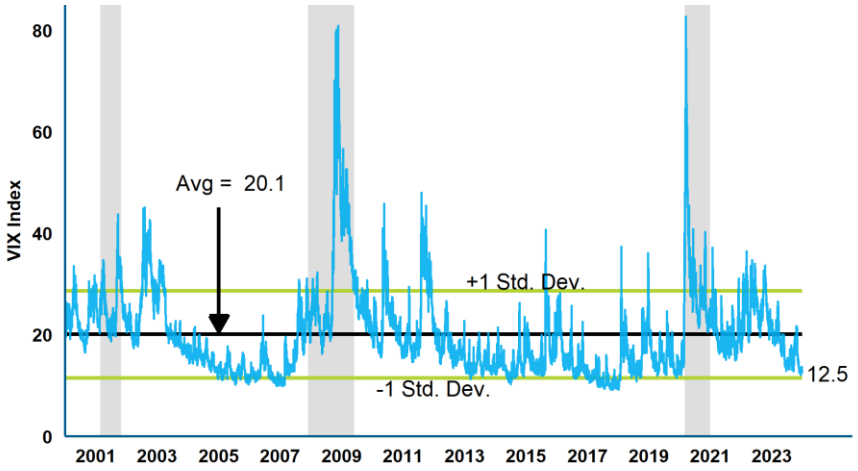


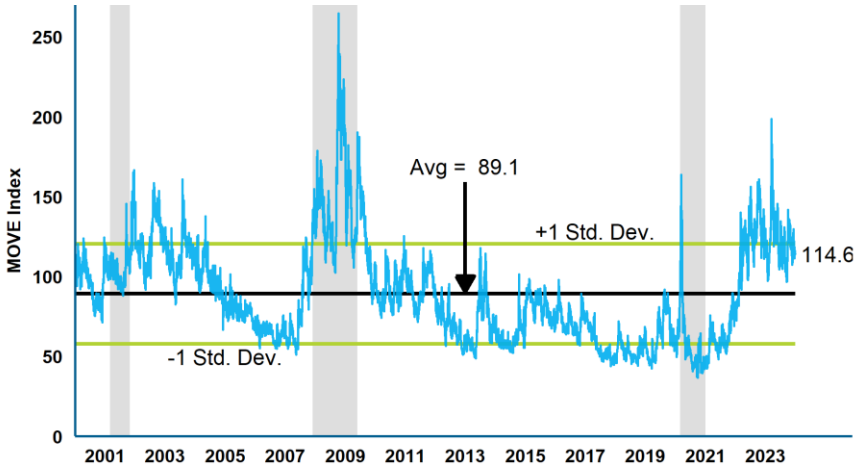
→ Expectations of peaking policy rates and the corresponding increase in risk appetite benefited credit in the fourth quarter with spreads (the added yield above a comparable maturity Treasury) narrowing. All spreads remain below their respective long run averages.

→ High yield spreads continue to be the furthest below their long-term average given the overall risk appetite last year and lower duration. Investment-grade corporate and emerging market spreads are also below their respective long-term averages, but by smaller margins.

[1] Sources: Bloomberg. Data is as of December 31, 2023. Average lines denote the average of the investment grade, high yield, and emerging market spread values from September 2002 to the recent month-end, respectively.

Equity and Fixed Income Volatility[1]



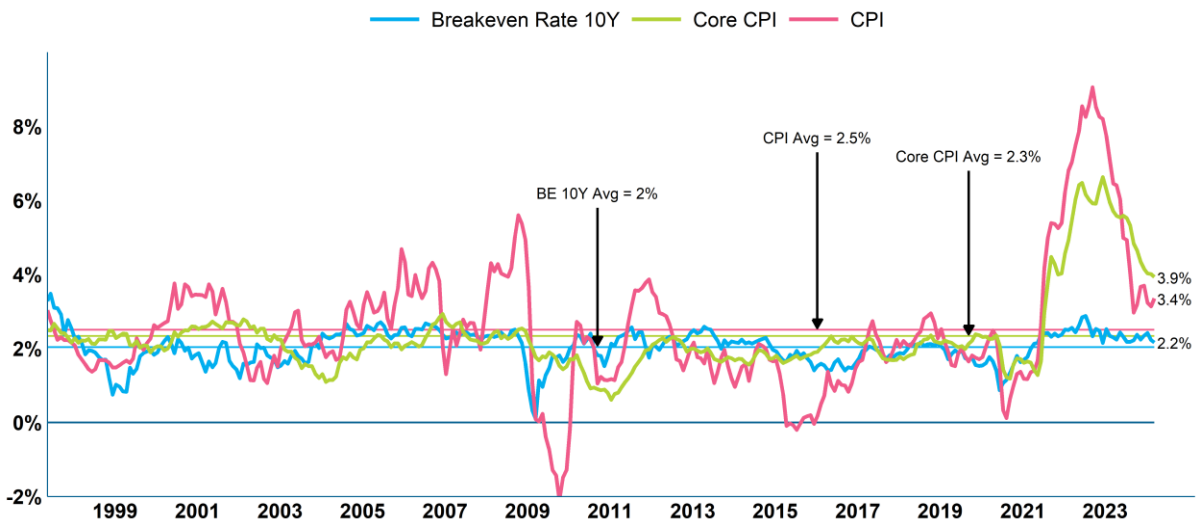


→ Volatility in equities (VIX) finished the year close to its lows, remaining well below the long-term average as the focus shifted to peaking policy rates and the potential for a soft landing.

→ Volatility in the bond market (MOVE) remained elevated to close out 2023 and is well above its long-run average (89.1). The bond market remained on edge for most of 2024 largely driven by uncertainty about the ultimate path of monetary policy.

[1] Equity Volatility – Source: FRED. Fixed Income Volatility – Source: Bloomberg. Implied volatility as measured using VIX Index for equity markets and the MOVE Index to measure interest rate volatility for fixed income markets. Data is as of December 2023. The average line indicated is the average of the VIX and MOVE values between January 2000 and December 2023.

US Ten-Year Breakeven Inflation and CPI[1]



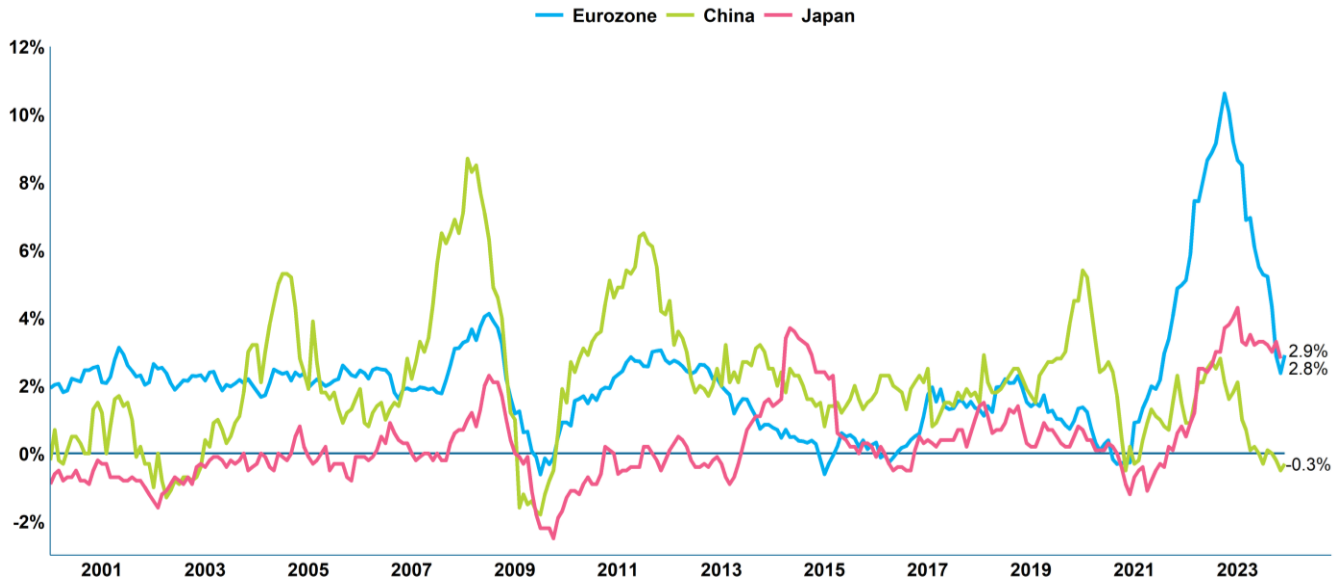
→ Year-over-year headline inflation rose from 3.1% to 3.4% in December, coming in above expectations of 3.2%. An increase in shelter (+6.2%) drove results, with food also increasing from a year prior (+2.7%) and energy prices falling (-2.0%). Month-over-month inflation came in at 0.3%, above expectations of 0.2% and the prior reading of 0.1%.

→ Core inflation - excluding food and energy – declined in December (3.9% versus 4.0%) year-over-year, with shelter costs again driving the total core index increase.

→ Inflation expectations (breakevens) have remained relatively stable despite the recent significant volatility in inflation.

[1] Source: FRED. Data is as December 2023. The CPI and 10 Year Breakeven average lines denote the average values from February 1997 to the present month-end, respectively. Breakeven values represent month-end values for comparative purposes.

Global Inflation (CPI Trailing Twelve Months)[1]



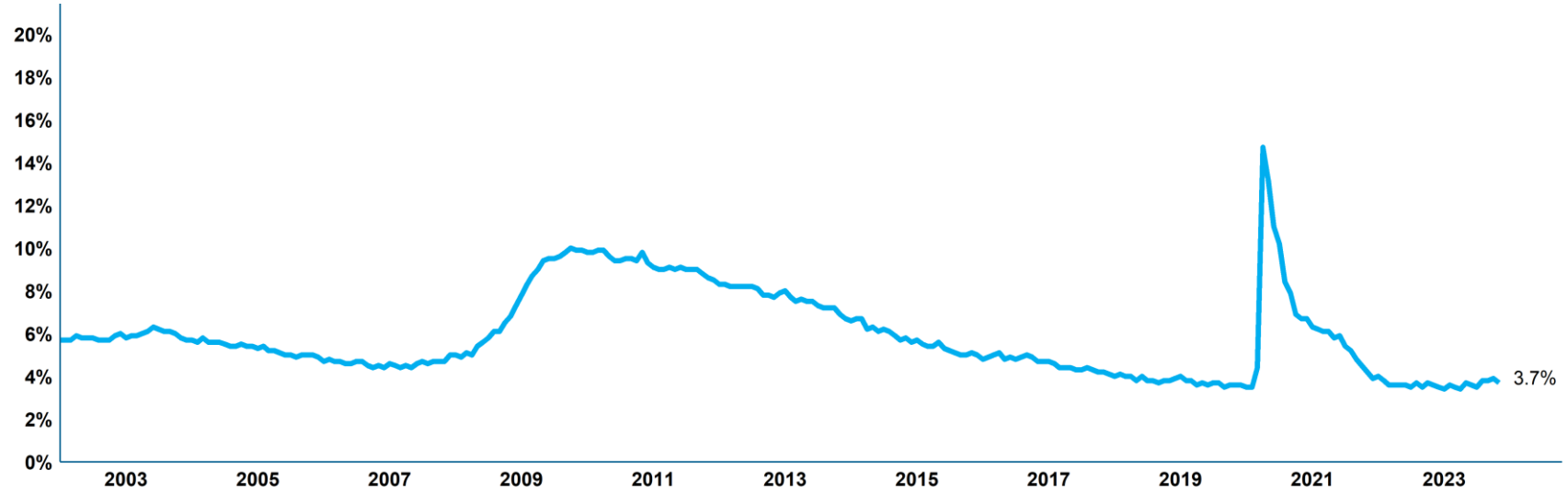
→ Outside the US, inflation is also falling across major economies with China slipping into deflation.

→ In the eurozone, inflation experienced a dramatic decline last year. Despite a small increase in December (2.9% versus 2.4%) it finished the year below the 3.4% year-over-year reading in the US.

→ Inflation in Japan remains near levels not seen in almost a decade, driven by food and home related items.

[1] Source: FRED for United States CPI and Eurozone CPI. Source: Bloomberg for Japan CPI, China CPI, and Eurozone December flash estimate. Data is as December 31, 2023, except Japan which is as of November 30, 2023.

US Unemployment[1]



→ Overall, the US labor market remains healthy with the unemployment rate relatively low, wage growth now positive in real terms, and initial claims for unemployment staying subdued.

→ In December, US unemployment remained unchanged (3.7%) and came in slightly below expectations of an increase to 3.8%. The number of jobs added did come in above expectations (216k versus 175k) though with the most jobs added in the government, leisure and hospitality, and health care sectors.

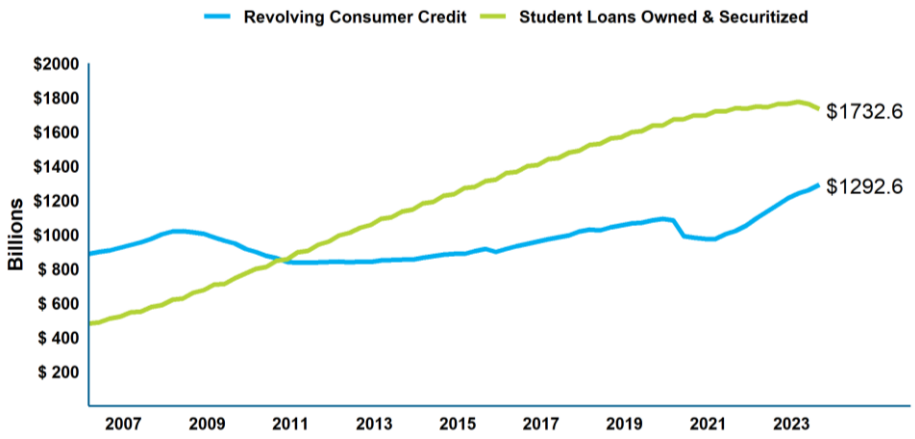
→ The labor force participation remained relatively stable at 62.5%, well off the lows of the pandemic (60.1%) but not back to pre-pandemic levels (63.3%).

→ The pace of hourly wage growth has declined from its peak of close to 6.0% finishing 2023 at 4.1% yoy. Wage growth remains positive in real terms though.

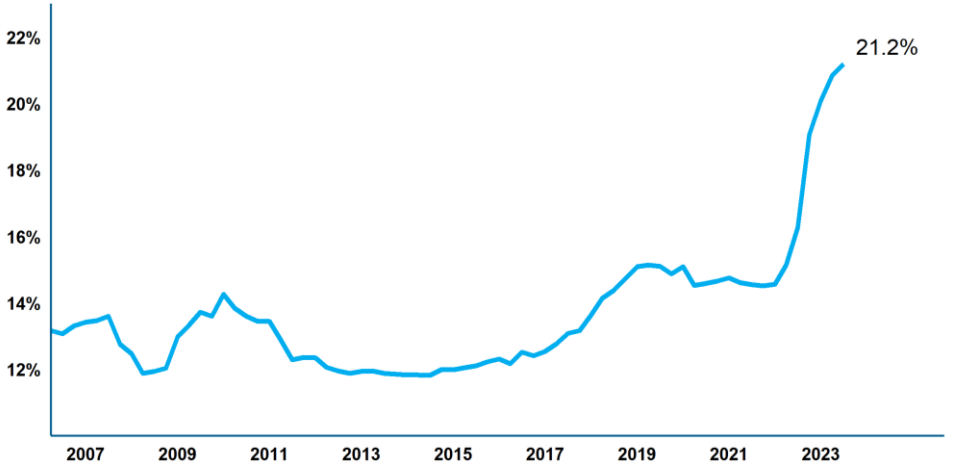
Source: FRED. Data is as December 31, 2023.

US Consumer Under Stress?[1]

Revolving Consumer Credit & Student Loans ($B)



Consumer Credit Card Interest Rates (%)



→ Despite the strong labor market and higher wages, pressures have started to build on the US consumer. This is an important consideration as consumer spending has been a key driver of economic growth.

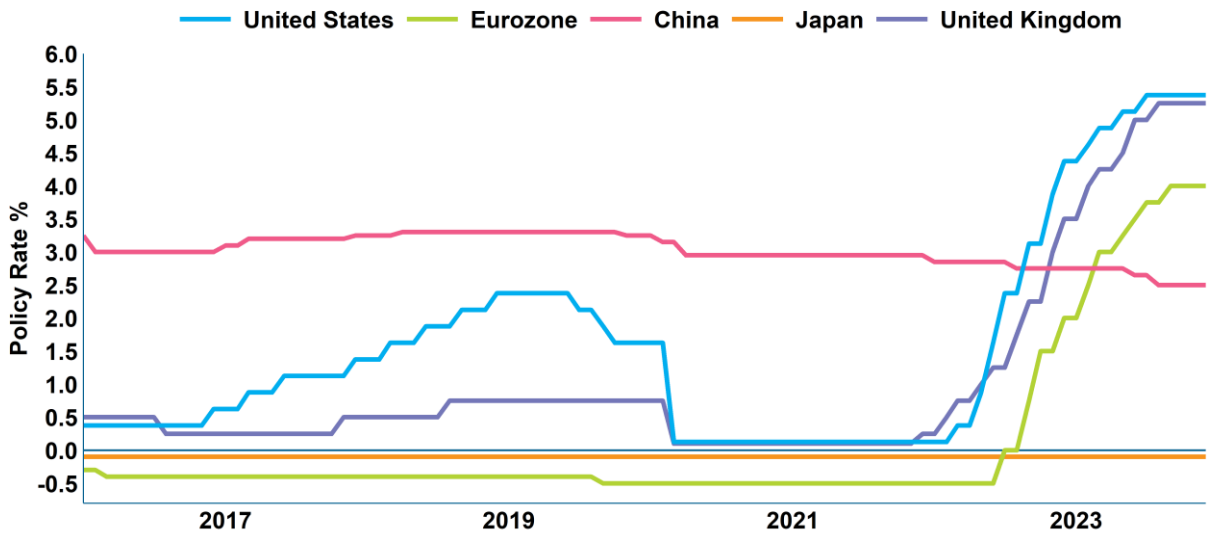
→ Revolving consumer credit surged to new highs in 2023 even as credit card interest rates hit levels not seen before (the prior peak was around 19% in the 1980s).

→ The return of student loan repayments after a three-year pandemic-related reprieve could add to pressures on consumers' budgets. This might be partially mitigated by recently initiated repayment and forgiveness programs.

→ As we look ahead, the strength of the US consumer will remain key as this sector makes up most of the domestic economy (GDP).

[1] Source: FRED. Data is as of September 30, 2023. Revolving Consumer Credit data is seasonally adjusted to remove distortions during the holiday season.

Policy Rates[1]



→ Slowing inflation and growth have led to expectations for a reduction in the pace of aggressive policy tightening.

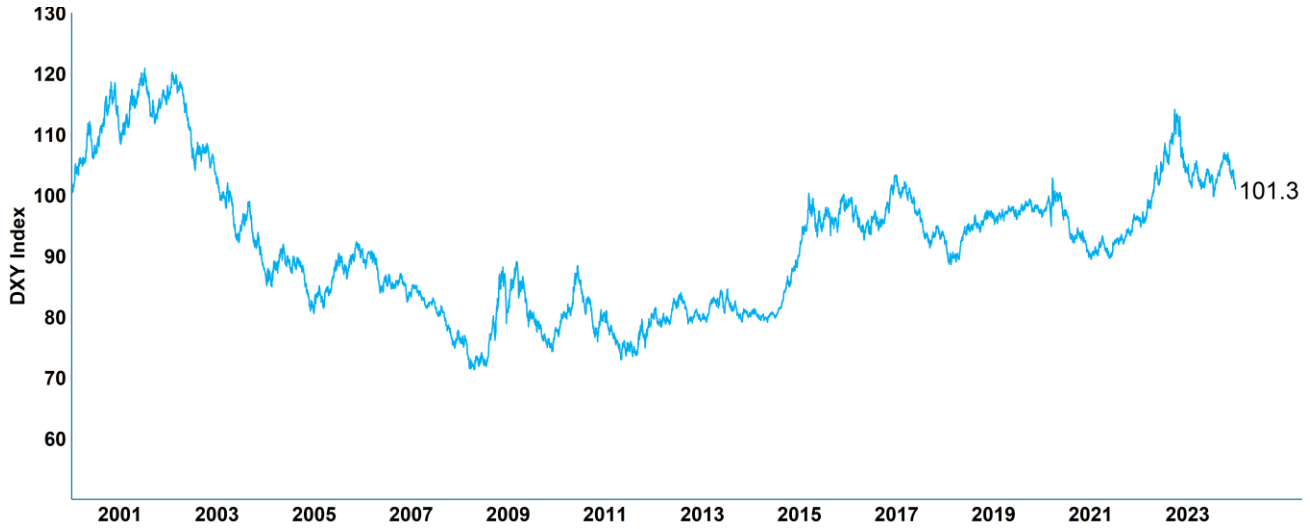
→ The Fed has been on hold since July 2023 when it raised rates to a range of 5.25%-5.50%. Markets are pricing in six rate cuts next year given the track of economic data and recent comments from the Fed, while the Fed itself is only predicting three. How this discrepancy is resolved will be key this year.

→ The European and UK central banks also recently paused their rate increases on slowing inflation. In Japan, the BoJ has further relaxed its yield curve control on the 10-year bond, and expectations for further policy normalization are rising.

→ The central bank in China has maintained interest rates at record low levels and continues to inject liquidity into the banking system, as weaker than expected economic data appears to indicate a widespread slowdown.

[1] Source: Bloomberg. Data is as of December 2023.

US Dollar vs. Broad Currencies[1]



→ The US dollar declined around 5% in the fourth quarter as generally weaker economic data led investors to anticipate the end of FOMC tightening and interest rate cuts in 2024.

→ Overall, the dollar finished the year only slightly below where it started but it was a volatile year for the US currency as expectations related to monetary policy evolved.

[1] Source: Bloomberg. Data as of December 31, 2023.

Summary

Key Trends:

→ The impact of inflation still above policy targets will remain important, with bond market volatility likely to stay high.

→ Global monetary policies could diverge going forward. The risk of policy errors remains elevated as central banks try to further reduce inflation toward targets while not tipping their economies into recession. In the case of the US the resolution of the disparity between market expectations for the path of interest rates versus the Fed's dot plot will be key.

→ Global growth is expected to slow next year, with some economies forecasted to tip into recession. However, optimism has been building that certain economies could experience soft landings. Inflation, monetary policy, and geopolitical issues will remain key in 2024.

→ US consumers could feel pressure as certain components of inflation (e.g., shelter), remain high, borrowing costs are elevated, and the job market may weaken.

→ A focus for US equities going forward, will be whether earnings can remain resilient if growth continues to slow. Also, the future paths of the large technology companies that have driven market gains will be important.

→ Equity valuations remain lower in emerging and developed markets, but risks remain, including the potential for China's economic slowdown and on-going weakness in the real estate sector could spill over into key trading partners' economies. Japan's recent hint at potentially tightening monetary policy along with changes in corporate governance in the country could influence relative results.

→ Recent, heightened tensions in Israel could add to overall uncertainty and drive safe haven flows.

Q4 Executive Summary

Performance Overview – Q4 2023

Total Market Value		Q4 Results		5 Year Results	
Q4 2023	$1,168,502,191	MercedCERA	6.0%	MercedCERA	9.3%
Q3 2023	$1,107,098,901	Policy Benchmark	5.8%	Policy Benchmark	9.7%

As of December 31, 2023, the value of the Fund's assets was $1,169 million.

→ The MercedCERA portfolio returned 6.0% for the quarter, outpacing its policy index by 30 basis points. This translates to annualized returns of 4.6%, 9.3% and 7.1% over the three, five and ten-year trailing periods. The portfolio's since inception annualized return is 8.0%.

→ Both equities and fixed income markets rallied in the fourth quarter of 2024, which contributed to all public asset classes in the portfolio returning strong absolute returns over the period. US Equities returned 11.9%, marginally trailing index return of 12.1%. Developed International Equity returned 9.5% over the period, trailing the benchmark by 90 basis points. Emerging Markets Equity posted 9.1% over the period, outpacing the benchmark by 120 basis points. US Fixed Income returned 7.0%, outperforming the index by 60 basis points. Opportunistic Credit also saw strong returns at 4.2% over the quarter, though trailing the blended benchmark by 170 basis points. Real Estate posted 2.8% for the quarter, outpacing the benchmark by 470 basis points. Private Equity saw marginal returns at 0.5%, compared to the (public market plus premium) index return of -2.7%. Real Assets returned 3.3%, trailing the index return of 7.2%.

→ Relative outperformance from Real Estate and Private Equity contributed over the quarter, though underperformance from Hedge Funds and Real Assets versus their respective benchmarks partially offset.

Public Manager Highlights Q4 2023

6 out of 13 Public Active Managers[1] either outperformed or matched their respective benchmarks for Q4 2023.

Total Equity (Active)

→ US Equity, returned 11.9%, trailing the benchmark (Russell 3000) by 20 basis points. BNY Mellon Newton Dynamic US Equity, MercedCERA's active large cap manager, matched their benchmark return of 11.7%. Champlain Small Cap, the portfolio's active small cap manager, returned 11.3%, trailing the index return of 14.0%. Underperformance was attributable to the fund's exclusion of the Real Estate sector, stock selection in Health Care and portfolio's underweight tilts in Financials and Consumer discretionary, the two strongest performing sectors over the period.

→ Developed International Equity returned 9.5%, trailing its benchmark by 90 basis points as despite strong absolute returns for all managers in the sleeve, only GQG International outpaced its benchmark. GQG outpaced its benchmark by 210 basis points as stock selection in the Utilities sector, underweight allocation to China as well as stock selection in India contributed. Of the three remaining managers, First Eagle performed the worst on both absolute and relative to benchmark basis, as the manager's value tilt was out of favor over the period.

→ Artisan & RWC, the two managers in the Emerging Markets space posted returns of 11.8% & 3.5% respectively. Relative to their index (MSCI Emerging Markets) return of 7.9%, Artisan materially outpaced the index, whereas RWC underperformed over the period. Artisan is a benchmark-agnostic strategy that invests in a small number of securities. Artisan cited positions in Ayden, cybersecurity firm Crowdstrike and Netflix as some of the strongest contributors over the quarter.

[1] Excludes Public Managers that do not have a full quarter of performance, Private Markets and Hedge Fund Managers.

Public Manager Highlights Q4 2023 (continued)

Total Fixed Income (Active)

→ US Fixed Income returned 7.0%, beating the benchmark by 60 basis points. Brandywine provided the strongest returns on both absolute (8.7%) and relative to benchmark basis (outpaced the Bloomberg US Aggregate by 1.9%), while Wellington Core Bond and Payden & Rygel Low Duration returned 7.3% and 2.8% respectively, with both funds outpacing their respective indices.

→ Opportunistic Credit returned 4.2%, trailing the blended benchmark return of 5.9%. Both PIMCO and GoldenTree funds posted positive absolute returns for the quarter, though PIMCO trailed relative to its benchmark. PIMCO Income Fund returned 5.9%, trailing its index by 6.8%, as exposures to non-Agency MBS, TIPS served as headwinds over the period.

Active Manager Expectations

Manager	Strategy Description	Beta (High/Neutral/Low)	Tracking Error Range (basis points)	Environments Manager Underperforms
Domestic Equity				
Champlain Small Cap	Moderately diversified small cap portfolio.	Low	4.0% to 7.0%	In low quality rallies.
Newton/Mellon Capital MCM Dynamic US Equity	Very diversified, quantitative, large cap core portfolio. Also has exposure to fixed income assets.	Neutral (higher in more recent periods)	2.5% to 5.0%	When investors misprice forward looking return/risk characteristics; when returns are concentrated in one sector.
Developed Markets Equity (Non-US)				
Driehaus International Small Cap Growth	Diversified growth manager that seeks to invest in companies experiencing positive growth inflections, using a combination of fundamental and macroeconomic analysis.	Low	4.0% to 7.0%	At market inflection points, with abrupt leadership change. Deep value, low quality market environments.
Acadian ACWI ex US Small Cap Equity	Very diversified international small cap portfolio, employing highly adaptive quantitative models.	Neutral	2.5% to 4.5%	During narrow markets, abrupt changes in leadership. In "value" challenged periods.
First Eagle International Value Fund	Benchmark agnostic, diversified international value manager with strategic gold allocation and willingness to utilize cash when valuations are elevated across the market.	Low	5.0% to 10.0%	In growth- and momentum-led rallies, where value discipline and an allocation to cash will be headwinds, and if physical gold underperforms.
GQG International Equity	Benchmark agnostic, concentrated international quality-growth equity manager with valuation discipline and macro awareness. Willing to invest in US-listed companies.	Low	5.0% to 10.0%	In cyclical recoveries where deep value, asset-heavy, smaller cap stocks rally.

Active Manager Expectations (continued)

Manager	Strategy Description	Beta (High/Neutral/Low)	Tracking Error Range (basis points)	Environments Manager Underperforms
Emerging Markets Equity				
Artisan Developing World	Concentrated, benchmark agnostic emerging markets strategy focused on high quality companies, overlaid with top-down macro (currency) awareness.	Neutral	5.0% to 10.0%	During cyclical rallies concentrated in deeper value, smaller cap stocks.
RWC Emerging Markets	Concentrated, growth-at-a-reasonable-price emerging markets equity strategy focused on mid cap stocks.	High	6.0% to 10.0%	Narrow rallies in large cap stocks where small and mid-caps lag, periods of heightened market volatility, deep drawdowns in asset-heavy cyclicals.
Investment Grade Bonds				
Brandywine	Top-down, macro, value-oriented strategy that invests with a benchmark agnostic philosophy	Neutral	2.0% to 7.0%	
Payden & Rygel	Short-term portfolios with emphasis on sector selection and yield curve management rather than relying on duration management	Low	0.2% to 0.7%	
Wellington	Benchmark-relative, diversified strategy with emphasis on individual security analysis, with Broad Markets teams' top-down sector views taken into consideration	Neutral	1.0 to 1.5%	
Opportunistic Credit				
PIMCO Income	Global multi-sector, benchmark agnostic approach, utilizing firm's resources to identify best income ideas while staying senior in the capital structure.	Low	1.5% to 3.5%	During periods of lower quality bond rallies and volatility in interest rates and certain currencies.
GoldenTree Multi-Sector Credit	Bottom-up security selection, managing risk and adding value through credit sector rotation.	Low	2.5% to 4.5%	During initial periods of economic recovery and rapid spread tightening.

Manager Monitor

Manager	Significant Events (Yes/No)	Last Meeting w Board of Retirement	Last Meeting with MIG	Comments
Domestic Equity Assets				
BNY Mellon Newton Dynamic US Equity Fund	No	-	June-23	Review of strategy, and discussion on current market environment.
Champlain Small Cap	No	-	Dec-23	Review of strategy & discussion of long-term management team succession plans, no changes to conviction level
Developed Markets Equity (Non-US) Assets				
Driehaus International Small Cap Growth	No	-	Oct-23	Review of strategy, no changes to conviction level. Regarding market outlooks, team somewhat bearish on China due to geopolitical concerns.
Acadian ACWI ex US Small Cap Equity	No	-	Feb- 23	Review of strategy, no changes to conviction level.
First Eagle International Value Fund	No		Mar-23	Review of strategy, no changes to conviction level
GQG International Equity	Yes	-	Jun-23	Discussion with management team regarding leadership turnover & non-US Equity strategies. Fund remains on Watch status.
Emerging Markets Equity Assets				
Artisan Developing World	No		Jun-23	Discussion around trend of increasing develop markets names exposure in portfolio. No major changes to conviction level.
RWC Emerging Markets	No	-	Oct-23	Review of strategy, no changes to conviction level.
US Fixed Income Assets				
Brandywine US Fixed Income	No	-	Mar-23	Review of strategy, no changes to conviction level
Payden & Rygel Low Duration	No	-	Aug-23	Review of strategy, no changes to conviction level
Wellington Core Bond	No	-	Mar-23	Review of strategy, no changes to conviction level
Opportunistic Credit				
PIMCO Income Fund	No	-	Dec-22	Discussion around impact of Portfolio Manager departure. No concerns after review.
GoldenTree Multi-Sector Credit	No	-	Mar-23	Review of strategy, no changes to conviction level.
Private Equity Program	N/A	N/A	N/A	Oversight by Cliffwater.
Real Assets Program	N/A	N/A	N/A	Oversight by Cliffwater.
Hedge Fund Program	N/A	N/A	N/A	Oversight by Cliffwater.

Active Manager Peer Rankings[1]

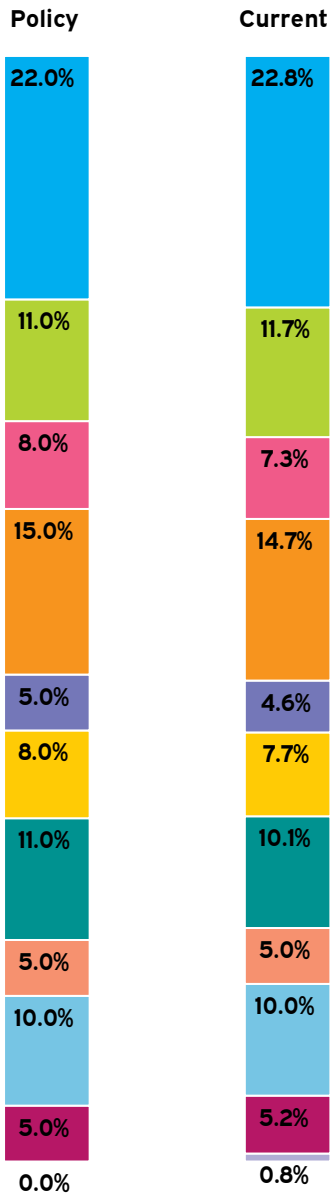
Investment Managers	Product	Peer Group	Market Value ($M)	1YR	3YR	5YR	10YR	Client Inception	Years in Portfolio
Champlain	Small Cap Fund	US Small Cap Core	30	74	96	88	58	Nov-20	3.1
Mellon Capital	Dynamic US Equity Strategy	US Large Cap Core	59	40	70	25	5	Dec-12	11.0
Acadian	All-Country World ex US Small Cap	Non-US Div Small Cap	15	66	26	13	26	May-19	4.6
Driehaus	International Small Cap Growth	ACWI ex US Small Cap Growth	15	73	57	23	32	May-19	4.6
GQG	International Equity	All ACWI ex US Equity	54	10	13	6	-	Dec-19	4.0
First Eagle	International Value	EAFE Value Equity	52	99	90	89	70	Dec-19	4.0
Artisan	Developing World	Emerging Markets	60	9	98	7	-	Dec-19	4.0
RWC	Emerging Markets	Emerging Markets	26	88	87	43	24	Dec-19	4.0
Brandywine	US Fixed Income	US Fixed Income	34	88	15	1	1	Nov-22	1.1
Payden & Rygel	Low Duration	US Short Duration Gov/Cred Fixed Income	8	24	42	40	42	Nov-22	1.1
Wellington	Core Bond	US Fixed Income	51	18	92	76	65	Nov-22	1.1
PIMCO	Income Fund	Global Multi-Sector Fixed Income	12	60	18	54	15	May-19	4.6
GoldenTree	Multi-Sector Credit Strategy	Global Multi-Sector Fixed Income	26	53	10	25	15	Jun-19	4.5

[1] Source: eVestment. Ranks are greyed out for periods before Merced CERA was invested.

Performance Update

As of December 31, 2023

Total Fund | As of December 31, 2023



Allocation vs. Targets and Policy

	Current Balance ($)	Current Allocation (%)	Policy (%)	Difference (%)	Policy Range (%)	Within IPS Range?
US Equity	266,653,863	22.8	22.0	0.8	16.0 - 27.0	Yes
International Equity	136,776,913	11.7	11.0	0.7	6.0 - 16.0	Yes
Emerging Markets Equity	85,699,629	7.3	8.0	-0.7	4.0 - 12.0	Yes
Private Equity	171,512,381	14.7	15.0	-0.3	5.0 - 20.0	Yes
Direct Lending	53,879,070	4.6	5.0	-0.4	0.0 - 10.0	Yes
Real Estate	89,464,324	7.7	8.0	-0.3	6.0 - 10.0	Yes
US Fixed Income	118,382,464	10.1	11.0	-0.9	6.0 - 16.0	Yes
Opportunistic Credit	58,973,417	5.0	5.0	0.0	3.0 - 7.0	Yes
Hedge Funds	116,574,012	10.0	10.0	0.0	5.0 - 15.0	Yes
Real Assets	61,193,690	5.2	5.0	0.2	3.0 - 7.0	Yes
Cash	9,392,428	0.8	0.0	0.8	0.0 - 5.0	Yes
Total	**1,168,502,191**	**100.0**	**100.0**	**0.0**		

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Total Fund (Net)	**1,168,502,191**	**100.0**	**6.0**	**4.7**	**11.7**	**4.6**	**9.3**	**7.1**	**8.0**	**Jan-95**
Total Fund (Gross)			**6.1**	**4.9**	**12.1**	**4.9**	**9.7**	**7.4**	**8.1**	**Jan-95**
Policy Index			*5.8*	*5.1*	*13.9*	*5.5*	*9.1*	*7.3*	*6.3*	
Total Fund w/o Alternatives (Net)	**666,486,285**	**57.0**	**9.5**	**5.8**	**17.0**	**2.1**	**9.5**	**6.9**	**--**	**Jan-08**
Total Fund w/o Alternatives (Gross)			**9.6**	**6.0**	**17.4**	**2.5**	**9.9**	**7.2**	**--**	**Jan-08**
Policy Index w/o AI			*9.5*	*6.0*	*15.7*	*2.4*	*8.2*	*6.3*	*--*	
US Equity (Net)	**266,653,863**	**22.8**	**11.9**	**7.7**	**24.6**	**8.0**	**14.6**	**11.5**	**10.3**	**Jan-95**
US Equity (Gross)			**12.0**	**7.8**	**24.8**	**8.2**	**14.9**	**11.8**	**10.4**	**Jan-95**
Russell 3000			*12.1*	*8.4*	*26.0*	*8.5*	*15.0*	*11.2*	*10.3*	
International Equity (Net)	**222,476,542**	**19.0**	**9.4**	**5.5**	**17.1**	**-2.0**	**9.9**	**5.0**	**5.6**	**Jan-99**
International Equity (Gross)			**9.6**	**5.9**	**18.1**	**-1.2**	**10.6**	**5.7**	**6.0**	**Jan-99**
International Equity Custom			*9.3*	*5.5*	*15.1*	*0.5*	*6.8*	*4.1*	*4.4*	
Developed International Equity (Net)	**136,776,913**	**11.7**	**9.5**	**6.9**	**14.8**	**3.9**	**9.5**	**4.8**	**4.4**	**Feb-08**
Developed International Equity (Gross)			**9.7**	**7.2**	**15.7**	**4.7**	**10.1**	**5.3**	**4.9**	**Feb-08**
Custom Blended Developed International Equity BM			*10.4*	*6.4*	*17.7*	*3.5*	*8.1*	*4.3*	*3.4*	
Emerging Markets Equity (Net)	**85,699,629**	**7.3**	**9.1**	**3.4**	**21.0**	**-10.8**	**9.0**	**5.2**	**4.7**	**May-12**
Emerging Markets Equity (Gross)			**9.4**	**3.9**	**22.2**	**-9.9**	**10.0**	**6.2**	**5.6**	**May-12**
MSCI EM			*7.9*	*4.7*	*9.8*	*-5.1*	*3.8*	*2.9*	*2.7*	
US Fixed Income (Net)	**118,382,464**	**10.1**	**7.0**	**3.5**	**5.0**	**-3.7**	**0.6**	**1.7**	**4.4**	**Jan-95**
US Fixed Income (Gross)			**7.0**	**3.5**	**5.1**	**-3.7**	**0.7**	**1.8**	**4.5**	**Jan-95**
US Fixed Income Custom Benchmark			*6.4*	*3.4*	*5.4*	*-3.0*	*1.0*	*1.8*	*4.6*	

Data Prior to March 2018 provided by prior consultant.

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Opportunistic Credit (Net)	**58,973,417**	**5.0**	**4.2**	**5.4**	**12.0**	**4.3**	**--**	**--**	**5.0**	**May-19**
Opportunistic Credit (Gross)			**4.3**	**5.7**	**12.7**	**4.8**	**--**	**--**	**5.4**	**May-19**
50% Barclays US Aggregate / 25% Barclays US High Yield / 25% Credit Suisse Lever			*5.9*	*5.2*	*9.4*	*0.2*	*--*	*--*	*2.5*	
Real Estate (Net)	**89,464,324**	**7.7**	**2.8**	**0.1**	**-2.6**	**4.5**	**2.9**	**5.4**	**6.6**	**Dec-10**
Real Estate (Gross)			**2.8**	**0.1**	**-2.6**	**4.5**	**2.9**	**5.8**	**7.5**	**Apr-99**
Custom Blended Real Estate Benchmark			*-1.9*	*-4.5*	*-12.1*	*7.1*	*5.4*	*7.4*	*7.1*	
CPI +5% (Seasonally Adjusted)			*1.7*	*4.1*	*8.5*	*10.9*	*9.3*	*7.9*	*7.7*	
Private Real Estate (Net)	**71,626,850**	**6.1**	**-0.4**	**-1.7**	**-5.7**	**5.3**	**3.3**	**5.6**	**6.7**	**Dec-10**
Private Real Estate (Gross)			**-0.4**	**-1.7**	**-5.7**	**5.4**	**3.3**	**6.0**	**7.6**	**Apr-99**
Custom Blended Real Estate Benchmark			*-1.9*	*-4.5*	*-12.1*	*7.1*	*5.4*	*7.4*	*7.1*	
Private Equity (Net)	**171,512,381**	**14.7**	**0.5**	**3.2**	**4.6**	**20.7**	**16.4**	**13.8**	**10.3**	**Jul-05**
Private Equity (Gross)			**0.5**	**3.2**	**4.6**	**20.7**	**16.4**	**13.9**	**10.4**	**Jul-05**
Custom Private Equity Benchmark			*-2.7*	*4.5*	*24.2*	*13.8*	*15.0*	*14.9*	*--*	
Direct Lending (Net)	**53,879,070**	**4.6**	**2.8**	**5.6**	**10.4**	**9.1**	**--**	**--**	**10.1**	**Jul-20**
Direct Lending (Gross)			**2.8**	**5.6**	**10.4**	**9.1**	**--**	**--**	**10.1**	**Jul-20**
S&P LSTA Leveraged Loan +2%			*3.4*	*7.5*	*15.6*	*7.9*	*7.9*	*6.5*	*9.4*	
Hedge Fund (Net)	**116,574,012**	**10.0**	**1.4**	**3.4**	**5.5**	**4.8**	**5.5**	**--**	**4.4**	**Jul-14**
Hedge Fund (Gross)			**1.8**	**4.1**	**6.7**	**5.8**	**6.4**	**--**	**4.9**	**Jul-14**
Custom Blended Hedge Fund Benchmark			*3.4*	*4.0*	*6.3*	*2.2*	*5.1*	*--*	*3.5*	
Real Assets (Net)	**61,193,690**	**5.2**	**3.3**	**4.8**	**11.3**	**14.1**	**12.0**	**9.5**	**9.7**	**Dec-10**
Real Assets (Gross)			**3.3**	**4.9**	**11.4**	**14.3**	**12.1**	**10.0**	**10.2**	**Dec-10**
Custom Blended Real Assets Benchmark			*7.2*	*5.2*	*5.6*	*9.4*	*7.9*	*7.1*	*--*	
CPI +5% (Seasonally Adjusted)			*1.7*	*4.1*	*8.5*	*10.9*	*9.3*	*7.9*	*7.8*	

Real Assets includes State Street Real Assets NL Fund.

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Private Infrastructure (Net)	**31,003,268**	**2.7**	**1.5**	**3.4**	**12.3**	**12.3**	**12.6**	**--**	**10.0**	**Jan-15**
Private Infrastructure (Gross)			**1.5**	**3.4**	**12.3**	**12.5**	**12.7**	**--**	**10.1**	**Jan-15**
S&P Global Infrastructure			*10.9*	*2.9*	*6.8*	*6.0*	*7.4*	*5.7*	*4.9*	
Private Natural Resources (Net)	**25,810,705**	**2.2**	**5.4**	**7.6**	**17.0**	**24.7**	**14.4**	**--**	**15.9**	**Oct-15**
Private Natural Resources (Gross)			**5.4**	**7.6**	**17.0**	**24.7**	**14.4**	**--**	**15.9**	**Oct-15**
S&P Global Natural Resources Sector Index (TR)			*3.6*	*7.4*	*4.1*	*12.9*	*11.1*	*5.1*	*11.3*	
Cash (Net)	**9,392,428**	**0.8**	**1.1**	**2.0**	**5.9**	**1.3**	**1.2**	**--**	**--**	**Dec-10**
Cash (Gross)			**1.1**	**2.0**	**5.9**	**1.3**	**1.2**	**--**	**--**	**Dec-10**

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Total Fund	**1,168,502,191**	**100.0**	**6.0**	**4.7**	**11.7**	**4.6**	**9.3**	**7.1**	**8.0**	**Jan-95**
Policy Index			*5.8*	*5.1*	*13.9*	*5.5*	*9.1*	*7.3*	*6.3*	
Total Fund w/o Alternatives	**666,486,285**	**57.0**	**9.5**	**5.8**	**17.0**	**2.1**	**9.5**	**6.9**	**--**	**Jan-08**
Policy Index w/o Al			*9.5*	*6.0*	*15.7*	*2.4*	*8.2*	*6.3*	*--*	
US Equity	**266,653,863**	**22.8**	**11.9**	**7.7**	**24.6**	**8.0**	**14.6**	**11.5**	**10.3**	**Jan-95**
Russell 3000			*12.1*	*8.4*	*26.0*	*8.5*	*15.0*	*11.2*	*10.3*	
BNY Mellon Newton Dynamic US Equity	58,763,014	5.0	11.7	7.4	24.2	8.3	15.9	13.2	15.3	Jan-13
S&P 500 Index			*11.7*	*8.0*	*26.3*	*10.0*	*15.7*	*12.0*	*13.7*	
BNY Mellon Large Cap	178,205,552	15.3	12.1	8.4	26.4	9.0	15.5	--	13.3	Apr-16
Russell 1000 Index			*12.0*	*8.4*	*26.5*	*9.0*	*15.5*	*11.8*	*13.3*	
Champlain Small Cap	29,685,296	2.5	11.3	3.8	14.1	0.8	--	--	7.9	Nov-20
Russell 2000 Index			*14.0*	*8.2*	*16.9*	*2.2*	*10.0*	*7.2*	*10.6*	
International Equity	**222,476,542**	**19.0**	**9.4**	**5.5**	**17.1**	**-2.0**	**9.9**	**5.0**	**5.6**	**Jan-99**
International Equity Custom			*9.3*	*5.5*	*15.1*	*0.5*	*6.8*	*4.1*	*4.4*	
Developed International Equity	**136,776,913**	**11.7**	**9.5**	**6.9**	**14.8**	**3.9**	**9.5**	**4.8**	**4.4**	**Feb-08**
Custom Blended Developed International Equity BM			*10.4*	*6.4*	*17.7*	*3.5*	*8.1*	*4.3*	*3.4*	
Acadian ACWI ex U.S. Small Cap Equity	15,483,688	1.3	9.4	7.7	13.7	5.8	--	--	9.1	May-19
MSCI AC World ex USA Small Cap (Net)			*10.1*	*8.3*	*15.7*	*1.5*	*7.9*	*4.9*	*5.7*	
Driehaus International Small Cap Growth	15,061,807	1.3	9.4	6.6	12.3	-1.2	--	--	8.0	May-19
MSCI AC World ex USA Small Growth Index (Net)			*10.2*	*6.1*	*14.1*	*-2.0*	*7.7*	*4.9*	*5.2*	
GQG International Equity	54,478,376	4.7	11.9	10.8	20.6	6.6	--	--	8.6	Dec-19
MSCI AC World ex USA (Net)			*9.8*	*5.6*	*15.6*	*1.5*	*7.1*	*3.8*	*4.8*	

Historical returns for the US Equity Composite prior to January 2012 and for the International Equity Composite prior to December 2010 are gross only.

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
First Eagle International Value Fund	51,753,042	4.4	7.2	2.8	10.0	2.3	--	--	3.5	Dec-19
MSCI EAFE (Net)			*10.4*	*5.9*	*18.2*	*4.0*	*8.2*	*4.3*	*5.7*	
Emerging Markets Equity	**85,699,629**	**7.3**	**9.1**	**3.4**	**21.0**	**-10.8**	**9.0**	**5.2**	**4.7**	**May-12**
MSCI EM			*7.9*	*4.7*	*9.8*	*-5.1*	*3.8*	*2.9*	*2.7*	
Artisan Developing World TR	59,666,787	5.1	11.8	3.8	29.3	-11.7	--	--	5.6	Dec-19
MSCI Emerging Markets (Net)			*7.9*	*4.7*	*9.8*	*-5.1*	*3.7*	*2.7*	*2.1*	
RWC	26,032,843	2.2	3.5	2.5	5.6	-8.5	--	--	0.7	Dec-19
MSCI Emerging Markets (Net)			*7.9*	*4.7*	*9.8*	*-5.1*	*3.7*	*2.7*	*2.1*	
US Fixed Income	**118,382,464**	**10.1**	**7.0**	**3.5**	**5.0**	**-3.7**	**0.6**	**1.7**	**4.4**	**Jan-95**
US Fixed Income Custom Benchmark			*6.4*	*3.4*	*5.4*	*-3.0*	*1.0*	*1.8*	*4.6*	
Vanguard Short-Term Treasury Index Fund	6,719,430	0.6	2.5	3.3	4.3	-0.1	1.2	--	1.4	Mar-18
Blmbg. 1-3 Govt			*2.6*	*3.3*	*4.3*	*-0.1*	*1.3*	*1.1*	*1.4*	
Vanguard Total Bond Market Index Fund	18,083,815	1.5	6.7	3.4	5.7	-3.3	--	--	0.6	May-19
Blmbg. U.S. Aggregate Index			*6.8*	*3.4*	*5.5*	*-3.3*	*1.1*	*1.8*	*0.5*	
Payden & Rygel Low Duration Fund	8,213,705	0.7	2.8	3.8	4.5	--	--	--	7.1	Nov-22
Blmbg. U.S. Treasury: 1-3 Year			*2.6*	*3.3*	*4.3*	*-0.1*	*1.3*	*1.0*	*4.4*	
Brandywine US Fixed Income	34,285,588	2.9	8.7	2.7	5.9	--	--	--	2.5	Nov-22
Blmbg. U.S. Aggregate Index			*6.8*	*3.4*	*5.5*	*-3.3*	*1.1*	*1.8*	*7.6*	
Wellington Core Bond	51,079,926	4.4	7.3	4.0	4.9	--	--	--	6.2	Nov-22
Blmbg. U.S. Aggregate Index			*6.8*	*3.4*	*5.5*	*-3.3*	*1.1*	*1.8*	*7.6*	

Developed International Equity and Emerging Markets Equity composites were only reported as one composite prior to March 2018.

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Opportunistic Credit	**58,973,417**	**5.0**	**4.2**	**5.4**	**12.0**	**4.3**	**--**	**--**	**5.0**	**May-19**
50% Barclays US Aggregate / 25% Barclays US High Yield / 25% Credit Suisse Lever			*5.9*	*5.2*	*9.4*	*0.2*	*--*	*--*	*2.5*	
PIMCO Income Fund	12,004,880	1.0	5.9	5.3	9.3	1.1	--	--	2.8	May-19
Blmbg. U.S. Aggregate Index			*6.8*	*3.4*	*5.5*	*-3.3*	*1.1*	*1.8*	*0.5*	
GoldenTree Multi-Sector Credit	25,803,657	2.2	5.1	7.3	12.8	4.4	--	--	5.2	Jun-19
50% BBg US High Yield TR/50% Credit Suisse Leveraged Loans			*5.0*	*7.0*	*13.3*	*3.9*	*5.5*	*4.5*	*4.6*	
Sculptor Credit Opportunities Domestic Partners, LP	392,565	0.0	0.0	0.0	11.0	7.8	--	--	9.5	Jul-20
50% BBg US High Yield TR/50% Credit Suisse Leveraged Loans			*5.0*	*7.0*	*13.3*	*3.9*	*5.5*	*4.5*	*6.0*	
OWS Credit Opportunity Fund LP	20,772,315	1.8	2.3	--	--	--	--	--	2.3	Oct-23
50% BBg US High Yield TR/50% Credit Suisse Leveraged Loans			*5.0*	*7.0*	*13.3*	*3.9*	*5.5*	*4.5*	*5.0*	
Real Estate	**89,464,324**	**7.7**	**2.8**	**0.1**	**-2.6**	**4.5**	**2.9**	**5.4**	**6.6**	**Dec-10**
Custom Blended Real Estate Benchmark			*-1.9*	*-4.5*	*-12.1*	*7.1*	*5.4*	*7.4*	*8.9*	
CPI +5% (Seasonally Adjusted)			*1.7*	*4.1*	*8.5*	*10.9*	*9.3*	*7.9*	*7.8*	
Vanguard REIT Index	17,837,475	1.5	18.1	8.1	11.8	5.0	--	--	6.5	Sep-20
Spliced Vanguard REIT Benchmark			*18.2*	*8.1*	*12.0*	*5.2*	*7.4*	*7.5*	*6.6*	
Private Real Estate	**71,626,850**	**6.1**	**-0.4**	**-1.7**	**-5.7**	**5.3**	**3.3**	**5.6**	**6.7**	**Dec-10**
Custom Blended Real Estate Benchmark			*-1.9*	*-4.5*	*-12.1*	*7.1*	*5.4*	*7.4*	*8.9*	
Greenfield Gap VII	913,260	0.1	2.6	5.4	-6.9	23.8	18.1	--	15.8	Jan-15
Patron Capital V	4,937,697	0.4	-7.5	-13.2	-2.9	-12.1	-8.8	--	-0.5	Feb-16
UBS Trumbull Property	23,171,993	2.0	-1.5	-5.1	-16.4	2.5	0.7	4.0	5.9	Apr-99
Carlyle Realty VIII	2,553,121	0.2	0.6	2.9	-5.0	41.4	26.7	--	10.4	Jan-18
Taconic CRE Dislocation Fund II	3,303,159	0.3	2.8	2.8	18.3	10.5	9.7	--	9.3	Nov-18

Sculptor market value reflects holdback from June liquidation.
All private markets performance and market values reflect a 9/30/2023 capital account balance unless otherwise noted.
Private Real Estate results prior to 1/1/2019 were included in the Real Assets composite. All results for the Private Real Estate composite that include the period prior to 1/1/2019 will reflect only the latest lineup of managers that Meketa received information for, therefore it may not reflect the entire Private Real Estate composite at that given time.

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Carmel Partners Investment Fund VII	4,149,910	0.4	-1.7	1.1	-0.2	-0.8	--	--	-19.3	Apr-19
AG Realty Value Fund X, L.P.	3,432,821	0.3	-1.4	-3.0	-3.9	12.9	--	--	5.1	Jun-19
Rockpoint Real Estate Fund VI, L.P.	4,594,861	0.4	-0.6	-2.1	-4.1	13.8	--	--	9.4	May-20
Cerberus Real Estate Debt Fund, L.P.	4,848,756	0.4	3.7	7.4	9.5	7.2	--	--	10.9	Jul-20
Taconic CRE Dislocation Onshore Fund III	6,192,808	0.5	5.0	5.6	7.4	--	--	--	7.8	Jun-21
Starwood Distressed Opportunity Fund XII Global	4,013,209	0.3	-5.1	-3.6	-7.4	--	--	--	97.1	Jun-21
Carlyle Realty Partners IX	1,391,161	0.1	2.7	4.5	-29.5	--	--	--	-154.9	Dec-21
Carmel Partners Investment Fund VIII	4,667,186	0.4	7.3	6.6	3.9	--	--	--	-5.8	Apr-22
Rockpoint Real Estate Fund VII L.P.	3,456,907	0.3	-2.9	-0.9	8.6	--	--	--	8.7	Aug-22
Private Equity	**171,512,381**	**14.7**	**0.5**	**3.2**	**4.6**	**20.7**	**16.4**	**13.8**	**10.3**	**Jul-05**
Custom Private Equity Benchmark			*-2.7*	*4.5*	*24.2*	*13.8*	*15.0*	*14.9*	*--*	
Taconic Credit Dislocation Fund IV L.P.	2,353,066	0.2	5.8	5.8	--	--	--	--	5.8	Jul-23
Khosla Ventures Seed F, L.P.	448,726	0.0	-3.8	-4.7	--	--	--	--	-4.7	Jul-23
Adams Street	3,735,169	0.3	-4.0	-3.8	-6.3	7.5	9.4	11.7	7.8	Oct-05
Invesco VI	477,377	0.0	-0.8	-10.0	-29.4	15.8	16.3	15.7	14.3	Jul-13
Ocean Avenue II	8,067,759	0.7	-8.9	-6.9	-14.9	38.7	28.8	--	20.2	Jul-14
Pantheon I	61,591	0.0	-1.5	-1.7	0.1	-10.3	-14.3	-4.4	-1.5	Jan-06
Pantheon II	2,685,109	0.2	-3.1	-2.1	-1.9	9.1	11.4	13.3	11.8	Jan-12
Pantheon Secondary	109,050	0.0	-0.6	-1.4	-1.5	-10.0	-7.7	-1.6	0.5	Jul-07

Pantheon I includes Pantheon US Fund VI and Pantheon Europe Fund IV. Pantheon Europe Fund IV is adjusting from the 12/31/2022 NAV.
Pantheon II includes Panthron US Fund IX, Pantheon Asia Fund VI, and Pantheon Europe Fund VII.
Pantheon Secondary includes Pantheon GLO SEC III B.
Adams Street includes Adams street 2005, Adams Street 2007, and Adams Street 2011.

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Davidson Kempner Long-Term Distressed Opportunities Fund IV	2,595,030	0.2	3.4	6.7	30.7	28.9	18.9	--	18.7	Apr-18
GTCR Fund XII	5,773,094	0.5	5.7	6.2	5.4	20.0	17.3	--	15.4	Jun-18
Carrick Capital Partners III	6,964,733	0.6	3.9	6.9	8.8	18.4	13.7	--	11.6	Aug-18
Cressey & Company Fund VI	5,244,612	0.4	-2.0	-1.5	2.1	18.8	14.7	--	14.7	Jan-19
TCV X	6,528,208	0.6	-3.7	4.9	6.9	18.9	--	--	16.7	Apr-19
Accel-KKR Growth Capital Partners III	4,782,037	0.4	2.8	-10.3	-6.0	15.3	--	--	6.6	Jul-19
Genstar Capital Partners IX	9,423,443	0.8	4.7	8.5	13.6	30.8	--	--	26.2	Aug-19
Cortec Group Fund VII	8,757,315	0.7	0.0	4.2	22.9	29.4	--	--	25.3	Dec-19
Spark Capital Growth Fund III	8,642,283	0.7	-1.7	-1.6	-26.4	22.7	--	--	14.4	Mar-20
Spark Capital VI	3,572,166	0.3	1.1	40.2	36.0	13.4	--	--	6.6	Mar-20
Summit Partners Growth Equity Fund X-A	8,644,810	0.7	1.5	3.2	14.5	5.5	--	--	6.7	Mar-20
Taconic Market Dislocation Fund III L.P.	7,216,666	0.6	1.6	6.6	8.4	16.7	--	--	14.1	Jul-20
Marlin Heritage Europe II, L.P.	7,459,164	0.6	-1.6	-1.1	13.3	-0.6	--	--	-0.5	Oct-20
Khosla Ventures VII	5,190,958	0.4	4.7	6.8	12.8	7.0	--	--	7.0	Jan-21
Accel-KKR Capital Partners VI	4,492,148	0.4	0.0	0.0	0.0	--	--	--	-4.7	Feb-21
Khosla Ventures Seed E	2,208,889	0.2	0.4	7.9	15.6	--	--	--	114.2	Feb-21
TCV XI	5,091,383	0.4	-3.6	-5.0	-9.0	--	--	--	-5.9	Feb-21
Thoma Bravo Discover Fund III	9,015,559	0.8	2.2	4.1	8.0	--	--	--	6.8	Jun-21

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Summit Partners Venture Capital Fund V-A	3,177,638	0.3	-1.4	3.5	4.5	--	--	--	-3.9	May-21
GTCR Fund XIII/A & B	4,211,387	0.4	2.7	5.5	1.0	--	--	--	81.6	Jun-21
Genstar Capital Partners X	7,656,469	0.7	1.2	-0.1	2.6	--	--	--	5.2	Oct-21
Nautic Partners X	3,591,915	0.3	7.2	12.7	20.1	--	--	--	6.7	Jan-22
Spark Capital Growth Fund IV	2,151,963	0.2	-1.9	-4.1	45.1	--	--	--	12.4	Jan-22
Spark Capital VII	1,374,145	0.1	-1.4	-3.3	-7.4	--	--	--	-7.3	Feb-22
TCV Velocity Fund I	3,833,228	0.3	2.5	61.7	46.6	--	--	--	0.4	Feb-22
Accel-KKR Growth Capital Partners IV	1,643,602	0.1	-0.1	0.8	2.0	--	--	--	-15.7	Apr-22
Summit Partners Growth Equity Fund XI-A	2,217,386	0.2	3.0	4.2	16.1	--	--	--	-40.5	Apr-22
GTCR Strategic Growth Fund I/A&B LP	1,662,342	0.1	5.7	6.3	-9.8	--	--	--	-34.7	Jul-22
Threshold Ventures IV LP	788,922	0.1	-3.9	-7.9	-19.6	--	--	--	-22.4	Aug-22
Thoma Bravo Discovery Fund IV	4,823,186	0.4	3.1	4.1	13.4	--	--	--	13.4	Jan-23
Marlin Heritage III	1,010,729	0.1	-5.4	-4.8	-84.0	--	--	--	-84.0	Jan-23
Cortec Group Fund VIII, L.P.	1,019,466	0.1	-9.2	-14.0	--	--	--	--	-14.9	Apr-23
Khosla Ventures VIII	407,034	0.0	-1.9	--	--	--	--	--	-1.9	Sep-23
Ares Capital Europe VI (D) Levered, L.P.	2,370,816	0.2	--	--	--	--	--	--	6.5	Nov-23
Genstar Capital Partners XI	31,809	0.0	--	--	--	--	--	--	0.0	Nov-23

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Direct Lending	**53,879,070**	**4.6**	**2.8**	**5.6**	**10.4**	**9.1**	**--**	**--**	**10.1**	**Jul-20**
S&P LSTA Leveraged Loan +2%			*3.4*	*7.5*	*15.6*	*7.9*	*7.9*	*6.5*	*9.4*	
Silver Point Specialty Credit Fund II, L.P.	6,709,340	0.6	2.8	5.5	12.4	9.5	--	--	10.4	Jul-20
Ares Senior Direct Lending Fund II	11,701,804	1.0	4.3	8.7	13.9	--	--	--	11.0	Jan-22
Varagon Capital Direct Lending Fund	13,054,558	1.1	2.8	5.0	5.8	--	--	--	2.4	Jan-22
AG Direct Lending Fund IV Annex	9,660,920	0.8	2.9	5.4	11.2	--	--	--	9.0	May-22
AG Direct Lending Fund V	4,743,635	0.4	2.4	3.9	9.9	--	--	--	8.1	Aug-22
Accel-KKR Credit Partners II LP	2,133,217	0.2	2.9	7.0	--	--	--	--	39.4	Mar-23
Silver Point Specialty Credit Fund III	5,875,597	0.5	0.0	1.5	--	--	--	--	-0.2	Mar-23
Hedge Fund	**116,574,012**	**10.0**	**1.4**	**3.4**	**5.5**	**4.8**	**5.5**	**--**	**4.4**	**Jul-14**
Custom Blended Hedge Fund Benchmark			*3.4*	*4.0*	*6.3*	*2.2*	*5.1*	*--*	*3.5*	
Hudson Bay Fund	15,474,092	1.3	0.4	2.9	--	--	--	--	3.2	Jun-23
Sculptor (OZ) Domestic II	264,914	0.0	-0.4	-0.6	6.7	-0.9	5.9	--	5.0	Jul-14
Graham Absolute Return	10,113,950	0.9	-1.5	5.0	3.1	7.7	5.9	--	4.6	Sep-17
Wellington-Archipelago	16,323,182	1.4	3.4	4.1	10.7	5.7	7.5	--	5.7	Sep-17
Marshall Wace Eureka	4,574,285	0.4	0.6	1.3	1.7	3.8	6.6	--	5.4	Dec-17
Silver Point Capital	19,074,926	1.6	2.1	1.8	5.8	10.4	9.7	--	7.9	Dec-17
Laurion Capital	13,945,606	1.2	1.6	3.7	5.4	3.8	9.2	--	9.1	Aug-18
Taconic Opportunity Fund	14,187,887	1.2	0.7	2.9	3.5	2.9	3.2	--	3.2	Jan-19

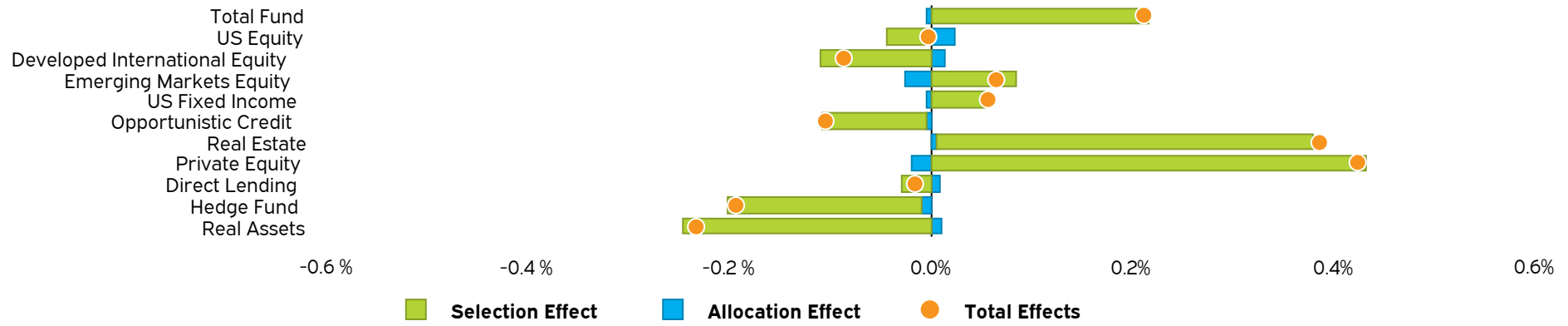
Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Marshall Wace Global Opportunities	10,990,429	0.9	0.5	2.3	6.3	1.5	--	--	5.3	May-20
Caxton Global Investments	11,624,741	1.0	3.3	6.7	-1.7	--	--	--	5.4	May-21
Real Assets	**61,193,690**	**5.2**	**3.3**	**4.8**	**11.3**	**14.1**	**12.0**	**9.5**	**9.7**	**Dec-10**
Custom Blended Real Assets Benchmark			*7.2*	*5.2*	*5.6*	*9.4*	*7.9*	*7.1*	*--*	
SSgA	4,379,717	0.4	3.4	2.6	0.6	7.3	7.6	--	5.5	May-17
Real Asset NL Custom Blended Index			*3.9*	*3.1*	*1.4*	*7.6*	*7.7*	*--*	*5.7*	
Private Infrastructure	**31,003,268**	**2.7**	**1.5**	**3.4**	**12.3**	**12.3**	**12.6**	**--**	**10.0**	**Jan-15**
S&P Global Infrastructure			*10.9*	*2.9*	*6.8*	*6.0*	*7.4*	*5.7*	*4.9*	
KKR Global II	3,426,301	0.3	2.3	4.3	22.2	21.4	22.1	--	16.8	Jan-15
North Haven Infrastructure II	2,619,297	0.2	-1.6	-2.0	-2.5	9.0	8.5	--	7.7	Jun-15
ISQ Global Infrastructure Fund II	5,502,231	0.5	1.4	3.0	8.6	12.6	13.1	--	4.3	Jul-18
KKR Global Infrastructure Investors III	4,533,851	0.4	4.4	6.7	17.9	3.3	-0.8	--	-0.8	Jan-19
Ardian Infrastructure Fund V	4,202,553	0.4	0.8	3.4	20.9	6.8	--	--	-7.4	Nov-19
ISQ Global Infrastructure Fund III	2,058,769	0.2	2.0	3.4	12.6	--	--	--	-494.2	Jun-21
KKR Global Infrastructure Investors IV	4,916,721	0.4	2.6	6.7	12.0	--	--	--	-220.0	Sep-21
BlackRock Global Infrastructure Fund IV	2,749,883	0.2	-1.9	-1.5	-13.6	--	--	--	-12.6	Dec-22
Ardian Infrastructure Fund VI	993,662	0.1								

Asset Allocation & Performance | As of December 31, 2023

	Market Value $	% of Portfolio	QTD (%)	Fiscal YTD	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	10 Yrs (%)	Inception (%)	Inception Date
Private Natural Resources	**25,810,705**	**2.2**	**5.4**	**7.6**	**17.0**	**24.7**	**14.4**	**--**	**15.9**	**Oct-15**
S&P Global Natural Resources Sector Index (TR)			*3.6*	*7.4*	*4.1*	*12.9*	*11.1*	*5.1*	*11.3*	
EnCap Flatrock Midstream Fund V	2,585,649	0.2	-1.1	-4.9	--	--	--	--	-4.9	Jun-23
EnCap XI	5,263,900	0.5	13.5	18.2	30.0	36.6	7.6	--	-4.6	Aug-17
EnCap IV	1,727,352	0.1	0.9	3.0	5.5	50.6	32.3	--	23.1	Mar-18
GSO Energy Opportunities	336,208	0.0	15.3	15.4	31.6	44.5	20.7	--	20.1	Dec-15
Taurus Mining	338,345	0.0	-5.1	-3.8	4.1	50.1	28.3	--	24.1	Oct-15
Taurus Mining Annex	176,371	0.0	-6.2	-4.9	2.0	18.5	19.6	--	22.8	Feb-17
BlackRock Global Energy and Power Infrastructure Fund III LP	4,410,346	0.4	-0.5	2.9	10.7	8.3	--	--	13.5	Aug-19
Tailwater Energy Fund IV, LP	3,632,718	0.3	-0.3	0.5	16.7	25.3	--	--	6.2	Oct-19
Carnelian Energy Capital IV	4,252,970	0.4	8.8	13.4	16.3	--	--	--	2.6	May-22
EnCap Energy Capital Fund XII	3,086,847	0.3	14.4	--	--	--	--	--	14.4	Aug-23
Cash	**9,392,428**	**0.8**	**1.1**	**2.0**	**5.9**	**1.3**	**1.2**	**--**	**--**	**Dec-10**
Cash	7,999,948	0.7	1.3	2.2	6.5	1.4	1.4	1.1	-1.3	Dec-10
Treasury Cash	1,392,480	0.1	0.0	0.0	0.0	0.0	0.0	--	0.1	Sep-17

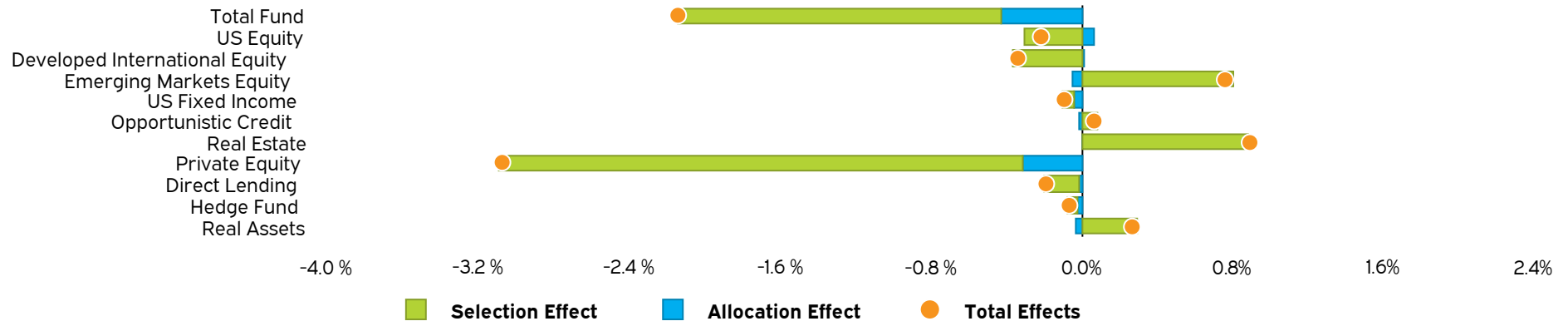
Attribution Effects
3 Months Ending December 31, 2023



Attribution Summary
3 Months Ending December 31, 2023

	Wtd. Actual Return (%)	Wtd. Index Return (%)	Excess Return (%)	Selection Effect (%)	Allocation Effect (%)	Total Effect (%)
US Equity	11.9	12.1	-0.1	0.0	0.0	0.0
Developed International Equity	9.5	10.4	-0.8	-0.1	0.0	-0.1
Emerging Markets Equity	9.1	7.9	1.2	0.1	0.0	0.1
US Fixed Income	7.0	6.4	0.6	0.1	0.0	0.1
Opportunistic Credit	4.2	5.9	-1.7	-0.1	0.0	-0.1
Real Estate	2.8	-1.9	4.7	0.4	0.0	0.4
Private Equity	0.5	-2.7	3.2	0.4	0.0	0.4
Direct Lending	2.8	3.4	-0.6	0.0	0.0	0.0
Hedge Fund	1.4	3.4	-2.0	-0.2	0.0	-0.2
Real Assets	3.3	7.2	-3.9	-0.2	0.0	-0.2
Total Fund	**6.0**	**5.8**	**0.2**	**0.2**	**0.0**	**0.2**

Attribution Effects
1 Year Ending December 31, 2023



Attribution Summary
1 Year Ending December 31, 2023

	Wtd. Actual Return (%)	Wtd. Index Return (%)	Excess Return (%)	Selection Effect (%)	Allocation Effect (%)	Total Effect (%)
US Equity	24.6	26.0	-1.4	-0.3	0.1	-0.2
Developed International Equity	14.8	17.7	-2.9	-0.4	0.0	-0.3
Emerging Markets Equity	21.0	9.8	11.2	0.8	-0.1	0.8
US Fixed Income	5.0	5.4	-0.4	-0.1	0.0	-0.1
Opportunistic Credit	12.0	9.4	2.6	0.1	0.0	0.1
Real Estate	-2.6	-12.1	9.5	0.9	0.0	0.9
Private Equity	4.6	24.2	-19.5	-2.8	-0.3	-3.1
Direct Lending	10.4	15.6	-5.2	-0.2	0.0	-0.2
Hedge Fund	5.5	6.3	-0.9	-0.1	0.0	-0.1
Real Assets	11.3	5.6	5.7	0.3	0.0	0.3
Total Fund	**11.7**	**13.9**	**-2.1**	**-1.7**	**-0.4**	**-2.1**

Benchmark History		
From Date	To Date	Benchmark
Total Fund		
01/01/2022	Present	22.0% Russell 3000, 11.0% Custom Blended Developed International Equity BM, 8.0% MSCI EM, 11.0% US Fixed Income Custom Benchmark, 10.0% Custom Blended Hedge Fund Benchmark, 15.0% Custom Private Equity Benchmark, 5.0% S&P LSTA Leveraged Loan +2%, 5.0% Custom Blended Real Assets Benchmark, 8.0% Custom Blended Real Estate Benchmark, 5.0% 50% Barclays US Aggregate / 25% Barclays US High Yield / 25% Credit Suisse Lever
01/01/2020	01/01/2022	21.0% Russell 3000, 10.0% Custom Blended Developed International Equity BM, 8.0% MSCI EM, 18.0% BBgBarc US Aggregate TR, 10.0% Custom Blended Hedge Fund Benchmark, 15.0% Custom Private Equity Benchmark, 5.0% Custom Blended Real Assets Benchmark, 8.0% Custom Blended Real Estate Benchmark, 5.0% 50% Barclays US Aggregate / 25% Barclays US High Yield / 25% Credit Suisse Lever
07/01/2019	01/01/2020	21.0% US Equity Custom, 18.0% International Equity Custom, 18.0% US Fixed Custom, 10.0% Custom Blended Hedge Fund Benchmark, 15.0% Thomson Reuters Cambridge Private Equity Index, 5.0% Real Asset Custom, 8.0% NCREIF ODCE (Net), 5.0% 50% Barclays US Aggregate / 25% Barclays US High Yield / 25% Credit Suisse Lever
01/01/2019	07/01/2019	21.0% US Equity Custom, 23.0% US Fixed Custom, 18.0% International Equity Custom, 10.0% Custom Blended Hedge Fund Benchmark, 15.0% Thomson Reuters Cambridge Private Equity Index, 5.0% Real Asset Custom, 8.0% NCREIF ODCE (Net)
01/01/2017	01/01/2019	27.0% US Equity Custom, 22.0% US Fixed Custom, 23.0% International Equity Custom, 5.0% Custom Blended Hedge Fund Benchmark, 9.0% Thomson Reuters Cambridge Private Equity Index, 14.0% Real Asset Custom
07/01/2014	01/01/2017	22.7% Russell 1000 Index, 5.7% Russell 2000 Index, 23.6% International Equity Custom, 28.5% US Fixed Custom, 4.5% Custom Blended Hedge Fund Benchmark, 8.0% NCREIF ODCE (Net), 7.0% Thomson Reuters Cambridge Private Equity Index
US Equity		
01/01/2020	Present	100.0% Russell 3000 Index
12/31/1994	01/01/2020	100.0% Russell 3000
International Equity		
01/01/2019	Present	56.0% MSCI EAFE Index, 44.0% MSCI Emerging Markets Index
01/01/2017	01/01/2019	69.6% MSCI EAFE Index, 30.4% MSCI Emerging Markets Index
07/01/2013	01/01/2017	100.0% MSCI AC World ex USA index
US Fixed Income		
12/01/1994	Present	10.0% Blmbg. U.S. Treasury: 1-3 Year, 90.0% BBgBarc US Aggregate TR

Benchmark History | As of December 31, 2023

From Date	To Date	Benchmark
Hedge Fund		
07/01/2017	Present	100.0% HFRI Fund of Funds Composite Index
01/01/2015	07/01/2017	50.0% HFRI Fund of Funds Composite Index, 50.0% HFRI RV: Multi-Strategy Index
Real Assets		
01/01/2022	Present	50.0% S&P Global Infrastructure, 50.0% S&P Global Natural Resources Sector Index (TR)
01/01/2020	01/01/2022	50.0% Cambridge Energy Upstream & Royalties & Private Energy (1 Quarter Lagged), 50.0% Cambridge Infrastructure (1 Quarter Lagged)
03/01/1999	01/01/2020	100.0% Real Asset Custom
SSgA		
04/01/2017	Present	10.0% S&P Global Infrastructure, 15.0% Dow Jones U.S. Select RESI, 25.0% Bloomberg Roll Select Commodity TR Index, 25.0% S&P Global LargeMidcap Resources & Commodities Ind, 25.0% Blmbg. U.S. TIPS
Private Real Estate		
01/01/2020	Present	100.0% NCREIF ODCE 1Q Lagged
03/01/1999	01/01/2020	100.0% NCREIF Fund Index-Open End Diversified Core Equity (VW) (Net)
Private Equity		
01/01/2022	Present	100.0% Custom PE BM (Jan 2022 -) 1Q Lag
01/01/2020	01/01/2022	100.0% Cambridge Global Private Equity & VC (1 Quarter Lagged)
12/31/1994	01/01/2020	100.0% Thomson Reuters Cambridge Private Equity Index

Annual Investment Expense Analysis

	Fee Schedule	Market Value	Estimated Annual Fee (%)	Estimated Expense
Total Fund		**1,168,502,191**		
Total Fund w/o Alternatives		**666,486,285**		
US Equity		**266,653,863**		
BNY Mellon Newton Dynamic US Equity	0.30 % of Assets	58,763,014	0.30	176,289
BNY Mellon Large Cap	0.04 % of First $100 M 0.02 % Thereafter	178,205,552	0.03	55,641
Champlain Small Cap	1.00 % of Assets	29,685,296	1.00	296,853
International Equity		**222,476,542**		
Developed International Equity		**136,776,913**		
Acadian ACWI ex U.S. Small Cap Equity	0.99 % of Assets	15,483,688	0.99	153,289
Driehaus International Small Cap Growth	0.90 % of Assets	15,061,807	0.90	135,556
GQG International Equity	0.50 % of Assets	54,478,376	0.50	272,392
First Eagle International Value Fund	0.79 % of Assets	51,753,042	0.79	408,849
Emerging Markets Equity		**85,699,629**		
Artisan Developing World TR	1.05 % of Assets	59,666,787	1.05	626,501
RWC	0.87 % of Assets	26,032,843	0.87	226,486
MCERA US FIXED+OPP CREDIT		**177,355,880**		
US Fixed Income		**118,382,464**		
Vanguard Short-Term Treasury Index Fund	0.05 % of Assets	6,719,430	0.05	3,360
Vanguard Total Bond Market Index Fund	0.04 % of Assets	18,083,815	0.04	6,329
Payden & Rygel Low Duration Fund	0.43 % of Assets	8,213,705	0.43	35,319
Brandywine US Fixed Income	0.29 % of Assets	34,285,588	0.29	99,428
Wellington Core Bond	0.12 % of Assets	51,079,926	0.12	61,296
Opportunistic Credit		**58,973,417**		
PIMCO Income Fund	0.51 % of Assets	12,004,880	0.51	61,225
GoldenTree Multi-Sector Credit	0.70 % of Assets	25,803,657	0.70	180,626
Sculptor Credit Opportunities Domestic Partners, LP	Performance Based 1.00 and 20.00	392,565	1.00	3,926

	Fee Schedule	Market Value	Estimated Annual Fee (%)	Estimated Expense
OWS Credit Opportunity Fund LP		20,772,315	-	-
Real Estate		**89,464,324**		
Vanguard REIT Index	0.10 % of Assets	17,837,475	0.10	17,837
Private Real Estate		**71,626,850**		
Greenfield Gap VII		913,260	-	-
Patron Capital V		4,937,697	-	-
UBS Trumbull Property		23,171,993	-	-
Carlyle Realty VIII		2,553,121	-	-
Taconic CRE Dislocation Fund II		3,303,159	-	-
Carmel Partners Investment Fund VII		4,149,910	-	-
AG Realty Value Fund X, L.P.		3,432,821	-	-
Rockpoint Real Estate Fund VI, L.P.		4,594,861	-	-
Cerberus Real Estate Debt Fund, L.P.		4,848,756	-	-
Taconic CRE Dislocation Onshore Fund III		6,192,808	-	-
Starwood Distressed Opportunity Fund XII Global		4,013,209	-	-
Carlyle Realty Partners IX		1,391,161	-	-
Carmel Partners Investment Fund VIII		4,667,186	-	-
Rockpoint Real Estate Fund VII L.P.		3,456,907	-	-
Private Equity		**171,512,381**		
Adams Street		3,735,169	-	-
Invesco VI		477,377	-	-
Ocean Avenue II		8,067,759	-	-
Pantheon I		61,591	-	-
Pantheon II		2,685,109	-	-
Pantheon Secondary		109,050	-	-
Davidson Kempner Long-Term Distressed Opportunities Fund IV		2,595,030	-	-
GTCR Fund XII		5,773,094	-	-
Carrick Capital Partners III		6,964,733	-	-
Cressey & Company Fund VI		5,244,612	-	-

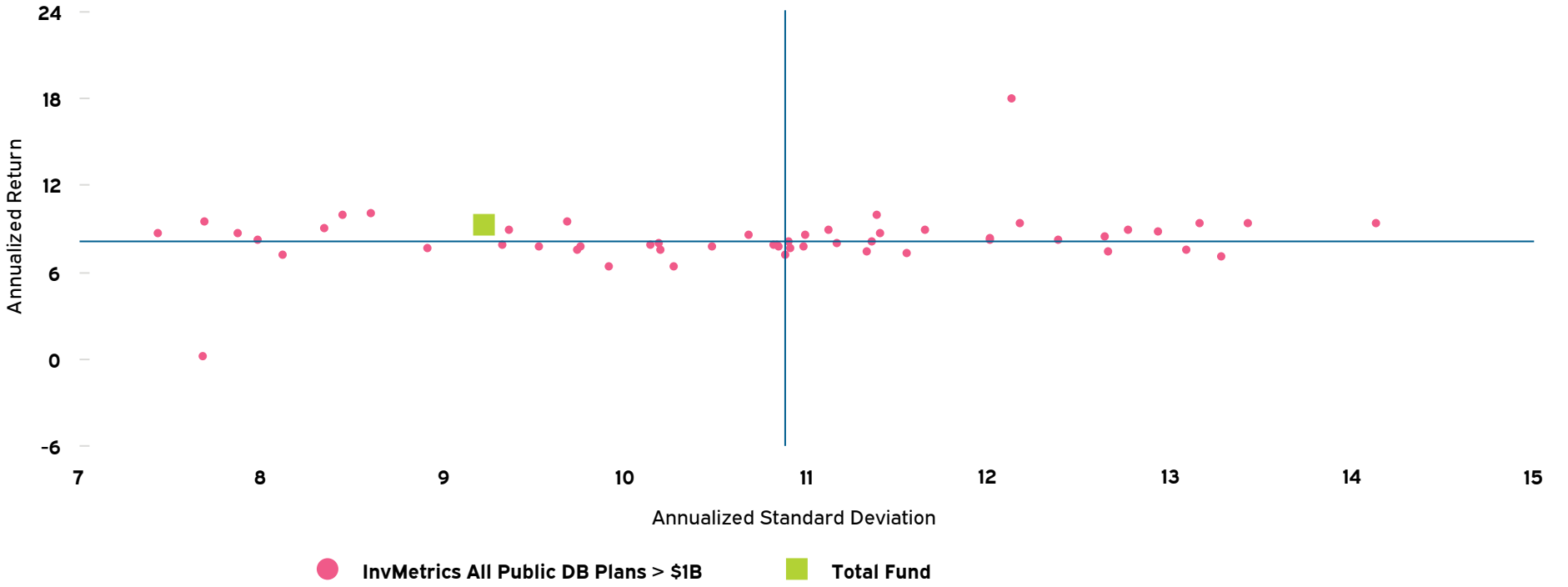
	Fee Schedule	Market Value	Estimated Annual Fee (%)	Estimated Expense
TCV X		6,528,208	-	-
Accel-KKR Growth Capital Partners III		4,782,037	-	-
Genstar Capital Partners IX		9,423,443	-	-
Cortec Group Fund VII		8,757,315	-	-
Spark Capital Growth Fund III		8,642,283	-	-
Spark Capital VI		3,572,166	-	-
Summit Partners Growth Equity Fund X-A		8,644,810	-	-
Taconic Market Dislocation Fund III L.P.		7,216,666	-	-
Marlin Heritage Europe II, L.P.		7,459,164	-	-
Khosla Ventures VII		5,190,958	-	-
Accel-KKR Capital Partners VI		4,492,148	-	-
Khosla Ventures Seed E		2,208,889	-	-
TCV XI		5,091,383	-	-
Thoma Bravo Discover Fund III		9,015,559	-	-
Summit Partners Venture Capital Fund V-A		3,177,638	-	-
GTCR Fund XIII/A & B		4,211,387	-	-
Genstar Capital Partners X		7,656,469	-	-
Nautic Partners X		3,591,915	-	-
Spark Capital Growth Fund IV		2,151,963	-	-
Spark Capital VII		1,374,145	-	-
TCV Velocity Fund I		3,833,228	-	-
Accel-KKR Growth Capital Partners IV		1,643,602	-	-
Summit Partners Growth Equity Fund XI-A		2,217,386	-	-
GTCR Strategic Growth Fund I/A&B LP		1,662,342	-	-
Threshold Ventures IV LP		788,922	-	-
Thoma Bravo Discovery Fund IV		4,823,186	-	-
Marlin Heritage III		1,010,729	-	-
Cortec Group Fund VIII, L.P.		1,019,466	-	-
Khosla Ventures VIII		407,034	-	-

Fee Schedule | As of December 31, 2023

	Fee Schedule	Market Value	Estimated Annual Fee (%)	Estimated Expense
Direct Lending		**53,879,070**		
Silver Point Specialty Credit Fund II, L.P.		6,709,340	-	-
Ares Senior Direct Lending Fund II		11,701,804	-	-
Varagon Capital Direct Lending Fund		13,054,558	-	-
AG Direct Lending Fund IV Annex		9,660,920	-	-
AG Direct Lending Fund V		4,743,635	-	-
Accel-KKR Credit Partners II LP		2,133,217	-	-
Silver Point Specialty Credit Fund III		5,875,597	-	-
Hedge Fund		**116,574,012**		
Sculptor (OZ) Domestic II	Performance Based 1.50 and 20.00	264,914	1.50	3,974
Graham Absolute Return	Performance Based 1.75 and 20.00	10,113,950	1.75	176,994
Wellington-Archipelago	Performance Based 1.00 and 20.00	16,323,182	1.00	163,232
Marshall Wace Eureka	Performance Based 2.00 and 20.00	4,574,285	2.00	91,486
Silver Point Capital	Performance Based 1.50 and 20.00	19,074,926	1.50	286,124
Laurion Capital	Performance Based 2.00 and 20.00	13,945,606	2.00	278,912
Taconic Opportunity Fund	Performance Based 1.40 and 20.00	14,187,887	1.40	198,630
Marshall Wace Global Opportunities	Performance Based 2.00 and 20.00	10,990,429	2.00	219,809
Caxton Global Investments	Performance Based 1.95 and 22.50	11,624,741	1.95	226,682
Real Assets		**61,193,690**		
SSgA	0.30 % of First $50 M 0.27 % of Next $50 M 0.25 % Thereafter Minimum Fee: $20,000	4,379,717	0.46	20,000
Private Infrastructure		**31,003,268**		
KKR Global II		3,426,301	-	-
North Haven Infrastructure II		2,619,297	-	-
ISQ Global Infrastructure Fund II		5,502,231	-	-
KKR Global Infrastructure Investors III		4,533,851	-	-
Ardian Infrastructure Fund V		4,202,553	-	-

	Fee Schedule	Market Value	Estimated Annual Fee (%)	Estimated Expense
ISQ Global Infrastructure Fund III		2,058,769	-	-
KKR Global Infrastructure Investors IV		4,916,721	-	-
BlackRock Global Infrastructure Fund IV		2,749,883	-	-
Ardian Infrastructure Fund VI		993,662	-	-
Private Natural Resources		**25,810,705**		
EnCap XI		5,263,900	-	-
EnCap IV		1,727,352	-	-
GSO Energy Opportunities		336,208	-	-
Taurus Mining		338,345	-	-
Taurus Mining Annex		176,371	-	-
BlackRock Global Energy and Power Infrastructure Fund III LP		4,410,346	-	-
Tailwater Energy Fund IV, LP		3,632,718	-	-
Carnelian Energy Capital IV		4,252,970	-	-
EnCap Energy Capital Fund XII		3,086,847	-	-
Cash		**9,392,428**		
Cash		7,999,948	-	-
Treasury Cash		1,392,480	-	-

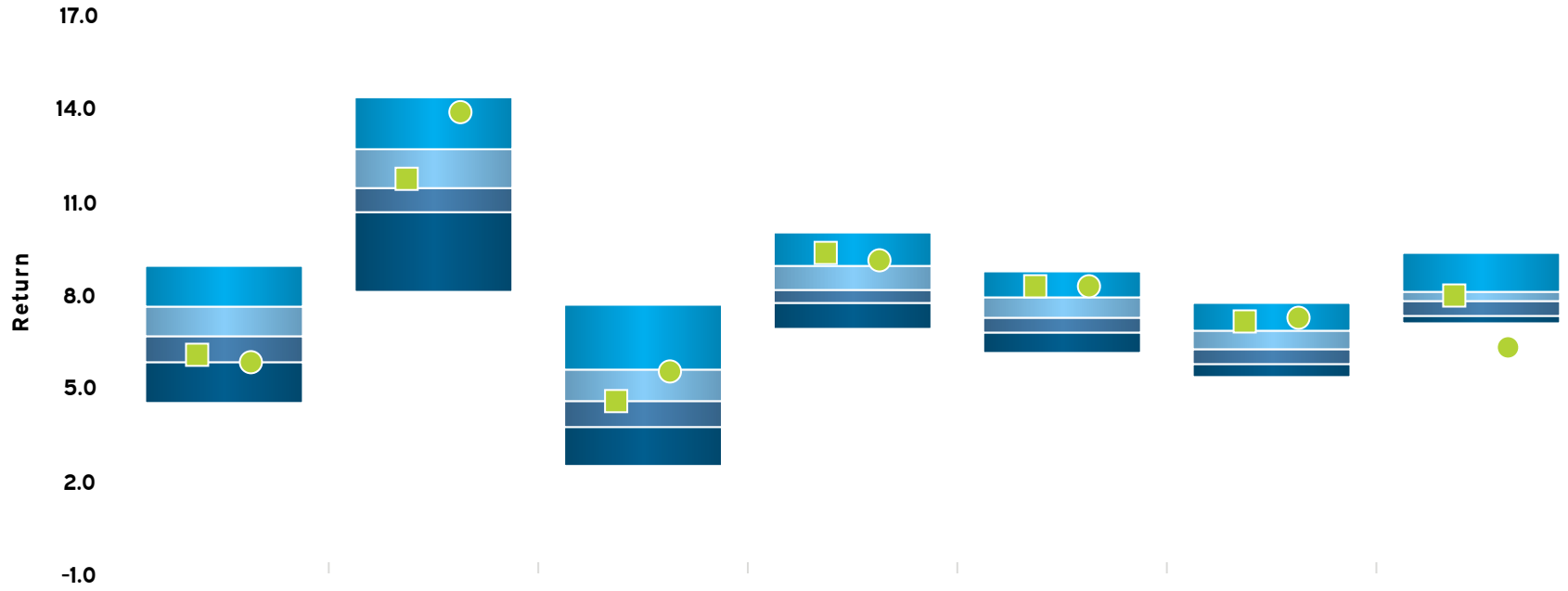
Annualized Return vs. Annualized Standard Deviation
5 Years Ending December 31, 2023



	5 Years Return	5 Years Standard Deviation	5 Years Information Ratio	5 Years Beta	5 Years Sharpe Ratio	5 Years Tracking Error
Total Fund	9.3 (18)	9.2 (18)	0.1 (17)	1.0 (22)	0.8 (13)	3.0 (4)
Policy Index	9.1 (19)	8.9 (17)	-	1.0	0.8 (13)	0.0
InvMetrics All Public DB Plans > $1B Median	8.1	10.9	-0.2	1.1	0.6	4.0

Statistics Summary 3 Years Ending December 31, 2023	5 Years Return	5 Years Standard Deviation	5 Years Information Ratio	5 Years Beta	5 Years Sharpe Ratio	5 Years Tracking Error
Total Fund	9.3	9.2	0.1	1.0	0.8	3.0
Policy Index	*9.1*	*8.9*	*-*	*1.0*	*0.8*	*0.0*
InvMetrics All Public DB Plans > $1B Median	8.1	10.9	-0.2	1.1	0.6	4.0

InvMetrics All Public DB Plans > $1B | As of December 31, 2023



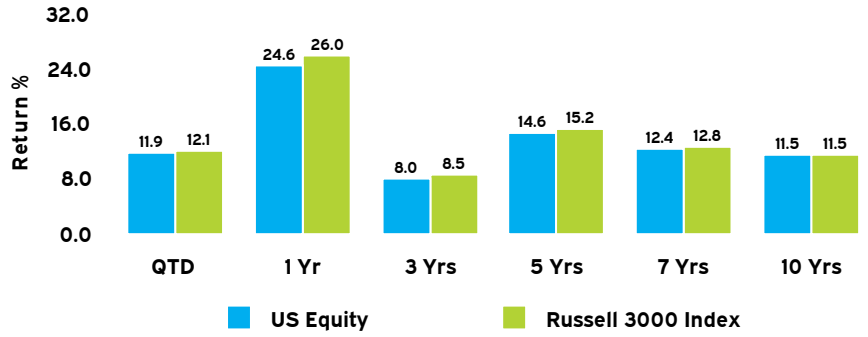
	QTD (%)	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)	Since Inception
Total Fund	6.0 (68)	11.7 (46)	4.6 (50)	9.3 (18)	8.2 (15)	7.1 (20)	8.0 (31)
Policy Index	5.8 (75)	13.9 (9)	5.5 (27)	9.1 (19)	8.2 (16)	7.3 (15)	6.3 (100)
5th Percentile	8.9	14.3	7.6	10.0	8.7	7.7	9.3
1st Quartile	7.6	12.6	5.6	8.9	7.9	6.8	8.1
Median	6.6	11.4	4.5	8.1	7.2	6.2	7.7
3rd Quartile	5.8	10.6	3.7	7.7	6.8	5.7	7.3
95th Percentile	4.5	8.0	2.4	6.9	6.1	5.3	7.0
Population	67	62	55	53	52	48	17

Parentheses contain percentile rankings.
Calculation based on monthly periodicity.

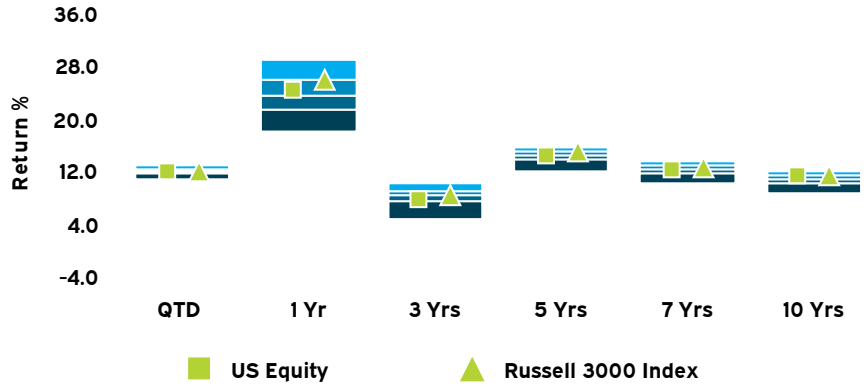
Merced County Employees' Retirement Association

US Equity | As of December 31, 2023

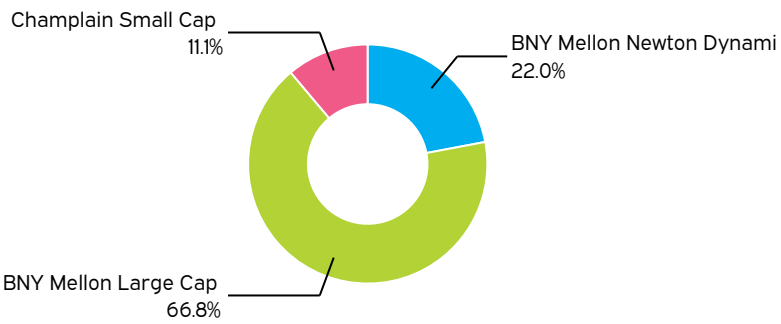
Return Summary



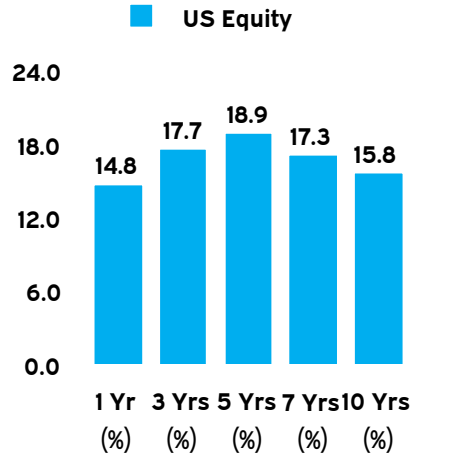
	QTD (%)	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
US Equity	11.9	24.6	8.0	14.6	12.4	11.5
Russell 3000	12.1	26.0	8.5	15.0	12.5	11.2
Excess Return	-0.2	-1.4	-0.5	-0.4	-0.1	0.3



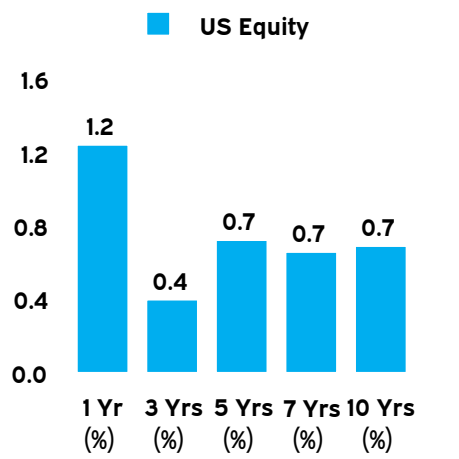
Current Allocation



Annualized Standard Deviation



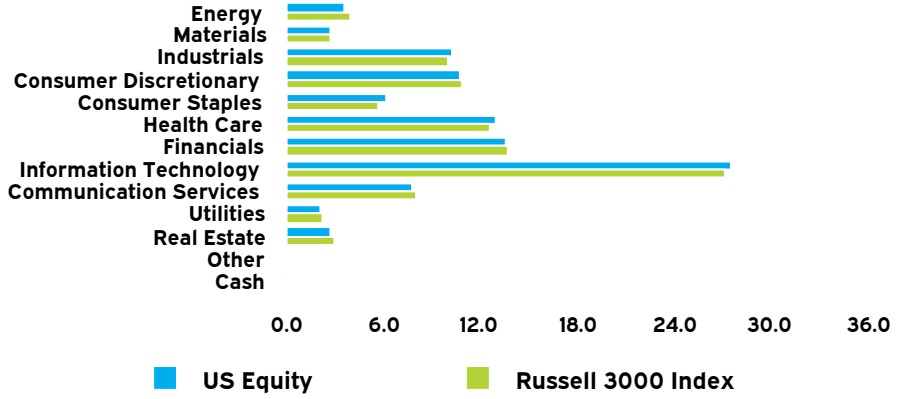
Sharpe Ratio



Equity Characteristics vs Russell 3000 Index

	Portfolio	Benchmark
Number of Holdings	1,071	2,976
Wtd. Avg. Mkt. Cap $B	612.9	618.1
Median Mkt. Cap $B	12.5	2.2
P/E Ratio	23.5	22.8
Yield (%)	1.4	1.5
EPS Growth - 5 Yrs. (%)	16.4	16.6
Price to Book	4.2	4.1

Sector Weights (%)



Top Holdings

Apple Inc	6.1
Microsoft Corp	6.0
Amazon.com Inc	2.9
NVIDIA Corporation	2.5
Alphabet Inc Class A	1.8
Meta Platforms Inc	1.7
Alphabet Inc Class C	1.5
Tesla Inc	1.5
Berkshire Hathaway Inc	1.4
JPMorgan Chase & Co	1.1
% of Portfolio	26.5

Ten Best Performers

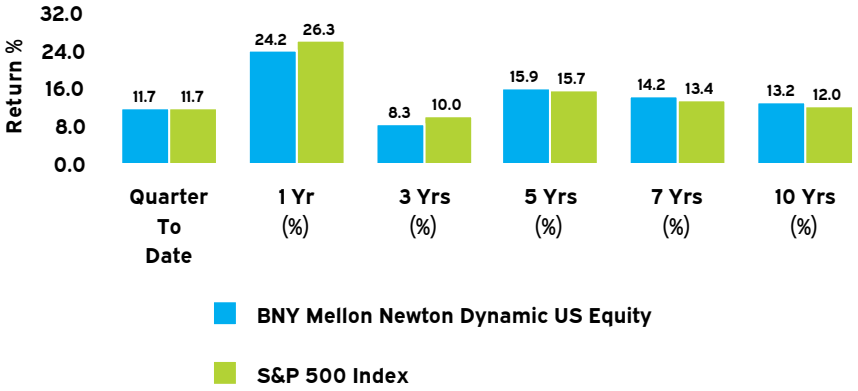
	Quarterly Return (%)
COINBASE GLOBAL INC	131.6
Affirm Holdings Inc	131.0
Gap Inc	99.6
Spirit Aerosystems Holdings Inc	96.9
Karuna Therapeutics Inc	87.2
Rocket Cos Inc	77.0
Block Inc	74.8
Macy's Inc	74.8
SentinelOne Inc	62.8
Frontier Communications Parent Inc	61.9

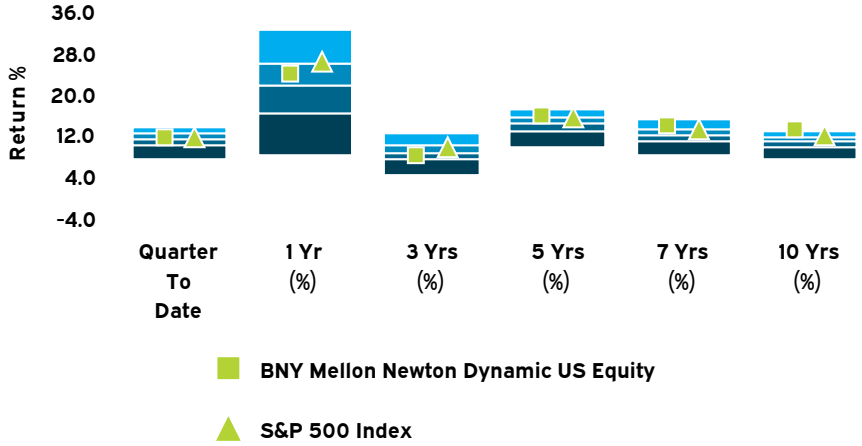
Ten Worst Performers

	Quarterly Return (%)
ChargePoint Holdings Inc	-52.9
Plug Power Inc	-40.8
James River Group Holdings Ltd	-39.5
Maravai LifeSciences Holdings Inc	-34.5
R1 RCM INC	-29.9
Agilon Health Inc	-29.3
BILL Holdings Inc	-24.8
Lucid Group Inc	-24.7
Hasbro Inc.	-21.6
Confluent Inc	-21.0

BNY Mellon Newton Dynamic US Equity | As of December 31, 2023

Return Summary





	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
BNY Mellon Newton Dynamic US Equity	11.7	24.2	8.3	15.9	14.2	13.2
S&P 500 Index	11.7	26.3	10.0	15.7	13.4	12.0
Excess Return	0.0	-2.1	-1.7	0.2	0.8	1.2

Annualized Standard Deviation

Sharpe Ratio

BNY Mellon Newton Dynamic US Equity | As of December 31, 2023

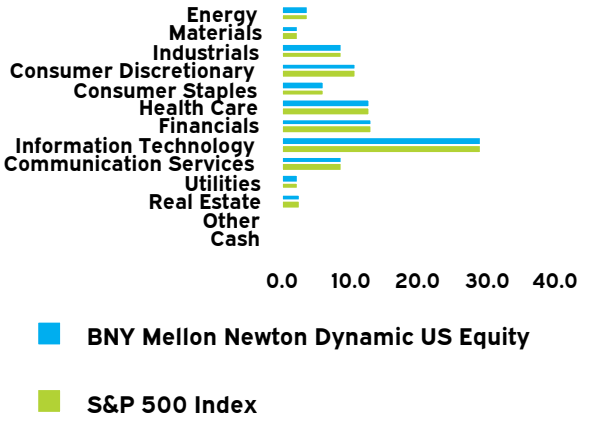
Equity Characteristics vs S&P 500 Index

	Portfolio	Benchmark
Number of Holdings	508	503
Wtd. Avg. Mkt. Cap $B	635.9	714.1
Median Mkt. Cap $B	33.4	33.5
P/E Ratio	24.0	24.0
Yield (%)	1.5	1.5
EPS Growth - 5 Yrs. (%)	16.9	16.9
Price to Book	4.4	4.4

Account Information

Account Name	BNY Mellon Newton Dynamic US Equity
Account Structure	Commingled Fund
Inception Date	11/30/2012
Asset Class	US Equity
Benchmark	S&P 500 Index
Peer Group	eV US Large Cap Core Equity

Sector Weights (%)



Top Holdings

Generic Fixed Income	10.9
Apple Inc	6.3
Microsoft Corp	6.2
Amazon.com Inc	3.1
NVIDIA Corporation	2.7
Alphabet Inc Class A	1.8
Meta Platforms Inc	1.7
Alphabet Inc Class C	1.6
Tesla Inc	1.5
Berkshire Hathaway Inc	1.4
% of Portfolio	37.2

Ten Best Performers

	Quarterly Return (%)
Expedia Group Inc	47.3
Advanced Micro Devices Inc	43.4
Intel Corp	41.8
D.R. Horton Inc	41.7
ProShares Ultra Semiconductors	41.4
Royal Caribbean Group	40.5
PulteGroup Inc	39.7
Fifth Third Bancorp	37.5
MarketAxess Holdings Inc	37.5
Monolithic Power Systems Inc	36.7

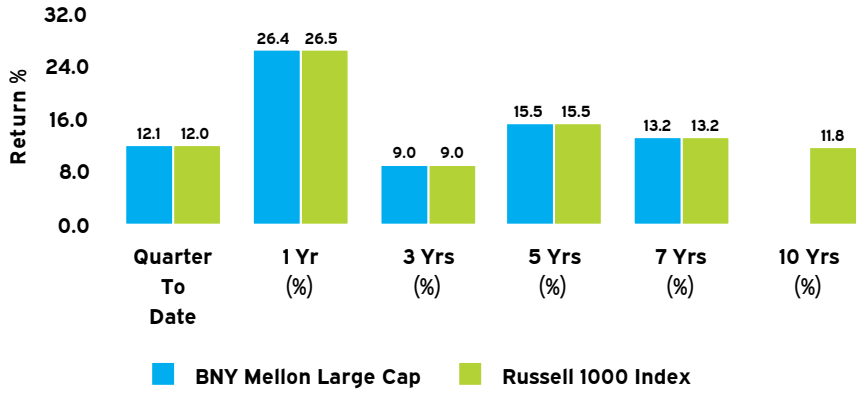
Ten Worst Performers

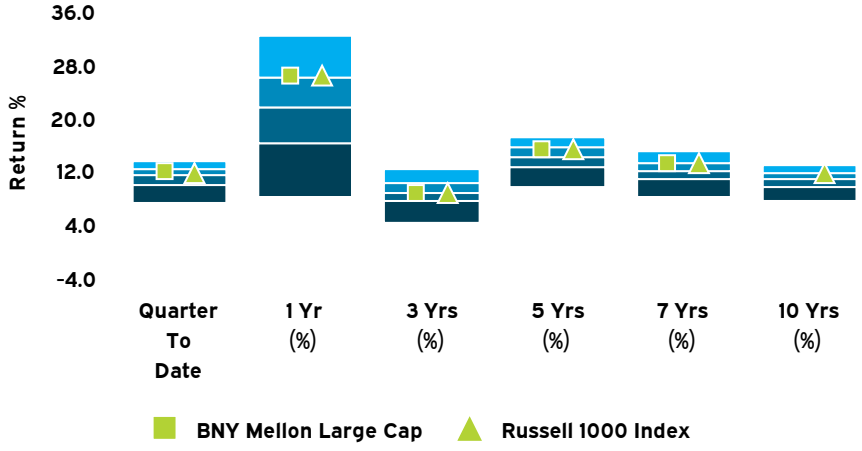
	Quarterly Return (%)
Hasbro Inc.	-21.6
Paycom Software Inc	-20.1
Hormel Foods Corp	-14.8
Albemarle Corp	-14.8
Exxon Mobil Corp	-14.2
APA Corporation	-12.2
Pfizer Inc	-12.0
Charter Communications Inc	-11.6
BorgWarner Inc	-10.9
Bristol-Myers Squibb Co	-10.7

Merced County Employees' Retirement Association

BNY Mellon Large Cap | As of December 31, 2023

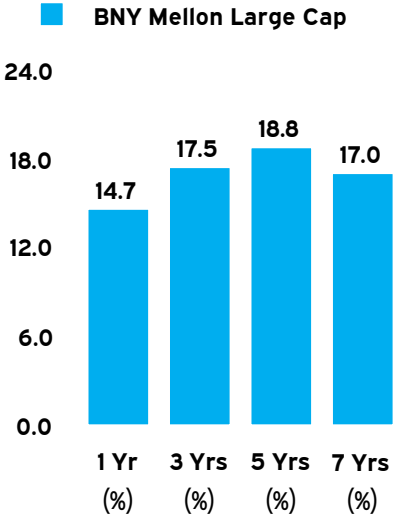
Return Summary





	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
BNY Mellon Large Cap	12.1	26.4	9.0	15.5	13.2	-
Russell 1000 Index	12.0	26.5	9.0	15.5	13.2	11.8
Excess Return	0.1	-0.1	0.0	0.0	0.0	-

Annualized Standard Deviation



Sharpe Ratio

BNY Mellon Large Cap | As of December 31, 2023

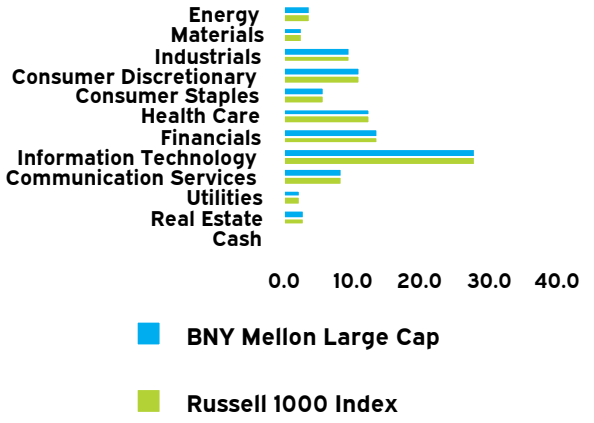
Equity Characteristics vs Russell 1000 Index

	Portfolio	Benchmark
Number of Holdings	1,008	1,010
Wtd. Avg. Mkt. Cap $B	652.3	653.3
Median Mkt. Cap $B	13.6	13.5
P/E Ratio	23.3	23.3
Yield (%)	1.5	1.5
EPS Growth - 5 Yrs. (%)	16.8	16.8
Price to Book	4.3	4.3

Account Information

Account Name	BNY Mellon Large Cap
Account Structure	Commingled Fund
Inception Date	03/31/2016
Asset Class	US Equity
Benchmark	Russell 1000 Index
Peer Group	eV US Large Cap Core Equity

Sector Weights (%)



Top Holdings

Apple Inc	6.5
Microsoft Corp	6.4
Amazon.com Inc	3.1
NVIDIA Corporation	2.7
Alphabet Inc Class A	1.9
Meta Platforms Inc	1.8
Alphabet Inc Class C	1.6
Tesla Inc	1.6
Berkshire Hathaway Inc	1.5
Eli Lilly and Co	1.1
% of Portfolio	28.2

Ten Best Performers

	Quarterly Return (%)
COINBASE GLOBAL INC	131.6
Affirm Holdings Inc	131.0
Gap Inc	99.6
Spirit Aerosystems Holdings Inc	96.9
Karuna Therapeutics Inc	87.2
Rocket Cos Inc	77.0
Block Inc	74.8
Macy's Inc	74.8
SentinelOne Inc	62.8
Frontier Communications Parent Inc	61.9

Ten Worst Performers

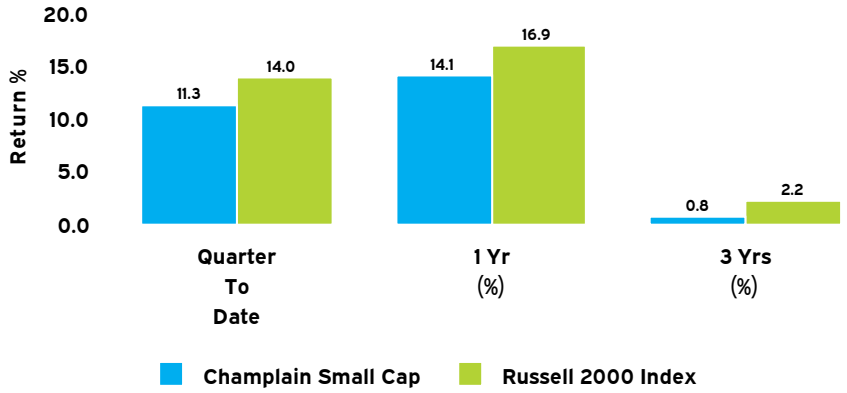
	Quarterly Return (%)
ChargePoint Holdings Inc	-52.9
Plug Power Inc	-40.8
Maravai LifeSciences Holdings Inc	-34.5
R1 RCM INC	-29.9
Agilon Health Inc	-29.3
BILL Holdings Inc	-24.8
Lucid Group Inc	-24.7
Hasbro Inc.	-21.6
Confluent Inc	-21.0
Maplebear Inc	-20.9

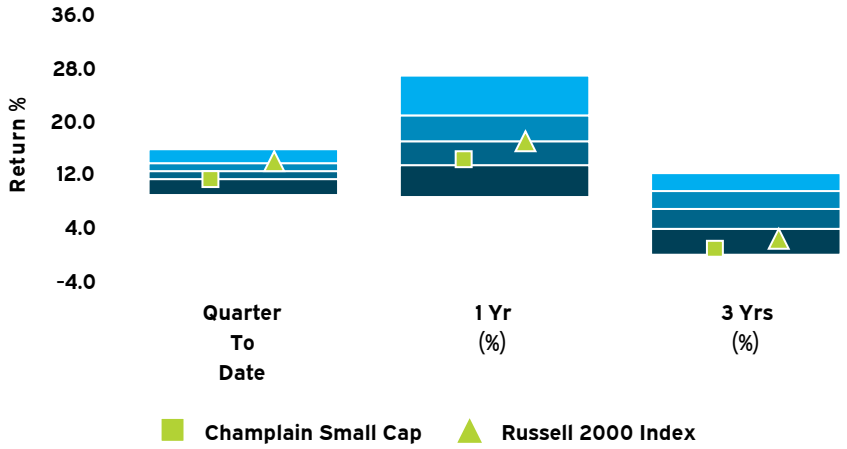
MEKETA

Merced County Employees' Retirement Association

Champlain Small Cap | As of December 31, 2023

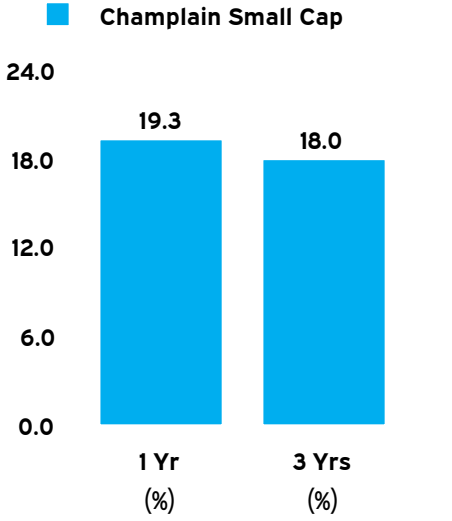
Return Summary



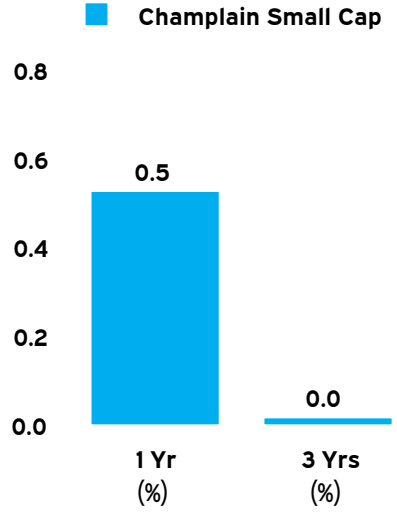


	Quarter To Date	1 Yr (%)	3 Yrs (%)
Champlain Small Cap	11.3	14.1	0.8
Russell 2000 Index	14.0	16.9	2.2
Excess Return	-2.7	-2.8	-1.4

Annualized Standard Deviation



Sharpe Ratio



Champlain Small Cap | As of December 31, 2023

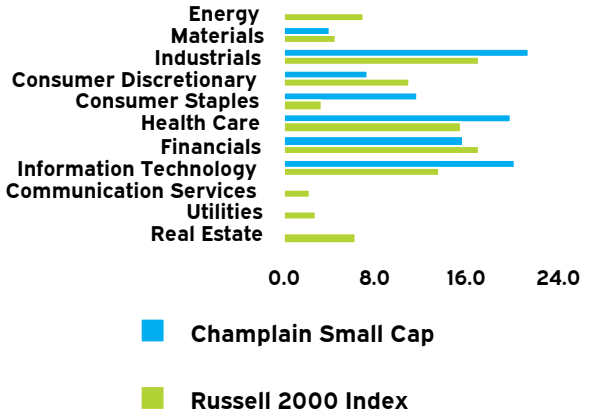
Equity Characteristics vs Russell 2000 Index

	Portfolio	Benchmark
Number of Holdings	73	1,966
Wtd. Avg. Mkt. Cap $B	4.5	3.2
Median Mkt. Cap $B	3.1	1.0
P/E Ratio	27.9	14.8
Yield (%)	0.6	1.5
EPS Growth - 5 Yrs. (%)	6.4	11.9
Price to Book	3.2	2.4

Account Information

Account Name	Champlain Small Cap
Account Structure	Mutual Fund
Inception Date	10/31/2020
Asset Class	US Equity
Benchmark	Russell 2000 Index
Peer Group	eV US Small Cap Core Equity

Sector Weights (%)



Top Holdings

Pure Storage Inc	3.2
RBC Bearings Inc	2.6
John Bean Technologies Corp	2.4
Freshworks Inc	2.4
Nutanix Inc	2.4
ESCO Technologies Inc.	2.3
Smartsheet Inc	2.2
Inspire Medical Systems Inc	2.2
Simply Good Foods Co (The)	2.1
Axonics Inc	2.0
% of Portfolio	23.8

Ten Best Performers

	Quarterly Return (%)
Sally Beauty Holdings Inc	58.5
Planet Fitness Inc	48.4
Bowlero Corp	47.2
Wingstop Inc	42.8
Tandem Diabetes Care Inc	42.4
Nutanix Inc	36.7
Independent Bank Corp.	35.2
Q2 Holdings Inc	34.5
Stock Yards Bancorp Inc	31.8
Freshpet Inc	31.7

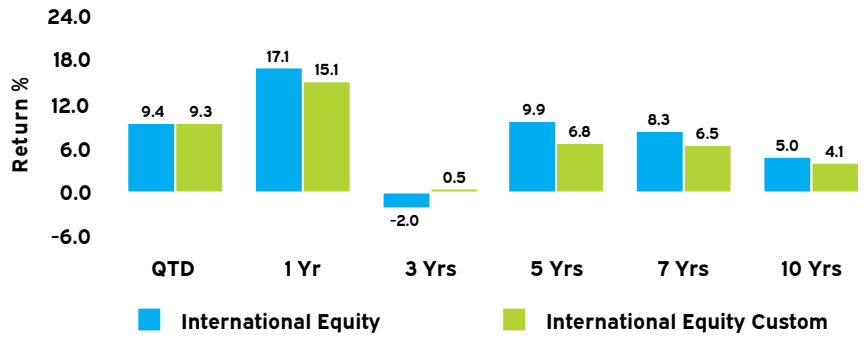
Ten Worst Performers

	Quarterly Return (%)
James River Group Holdings Ltd	-39.5
AtriCure Inc	-18.5
Omnicell Inc	-16.5
European Wax Center Inc	-16.1
MGP Ingredients Inc	-6.5
John Bean Technologies Corp	-5.3
Hayward Holdings Inc	-3.5
Barnes Group Inc	-3.4
Selective Insurance Group Inc	-3.2
Ollie's Bargain Outlet Holdings Inc	-1.7

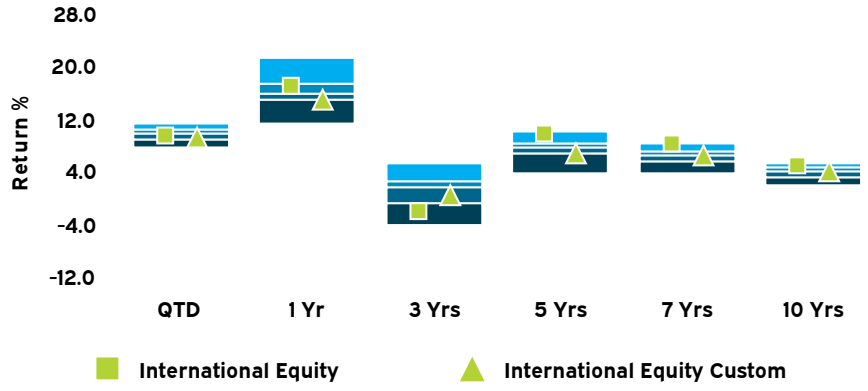
Merced County Employees' Retirement Association

International Equity | As of December 31, 2023

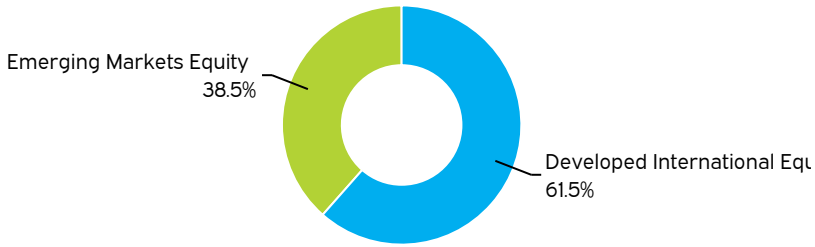
Return Summary



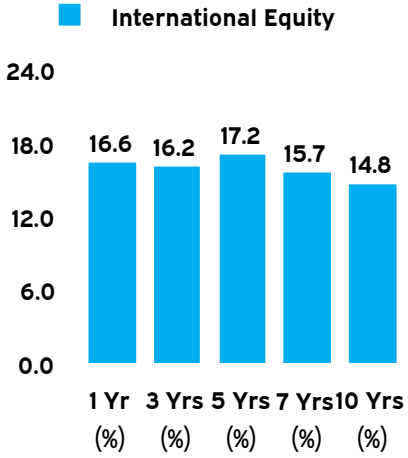
	QTD (%)	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
International Equity	9.4	17.1	-2.0	9.9	8.3	5.0
International Equity Custom	9.3	15.1	0.5	6.8	6.5	4.1
Excess Return	0.1	2.0	-2.5	3.1	1.8	0.9



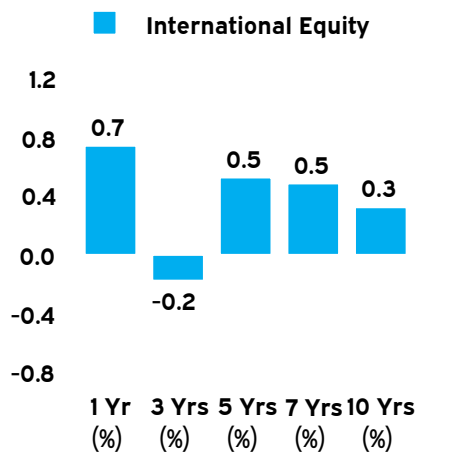
Current Allocation



Annualized Standard Deviation



Sharpe Ratio



MEKETA

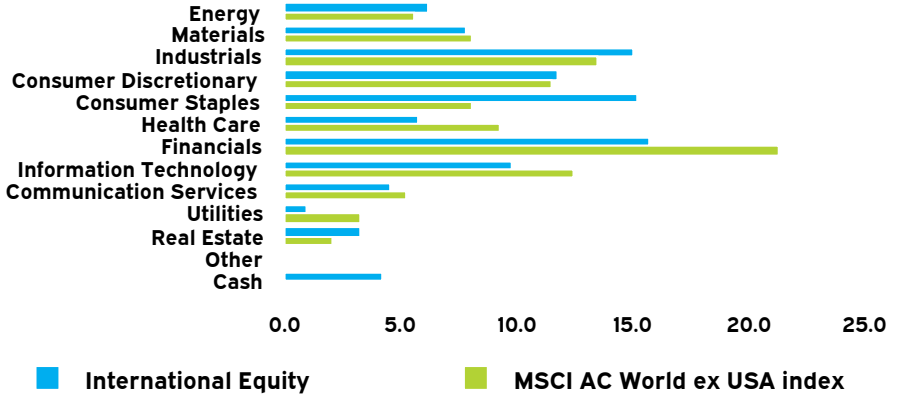
Merced County Employees' Retirement Association

International Equity | As of December 31, 2023

Equity Characteristics vs MSCI AC World ex USA index

	Portfolio	Benchmark
Number of Holdings	2,048	2,312
Wtd. Avg. Mkt. Cap $B	48.5	90.3
Median Mkt. Cap $B	0.7	9.8
P/E Ratio	13.1	13.6
Yield (%)	2.7	3.1
EPS Growth - 5 Yrs. (%)	12.6	10.4
Price to Book	2.2	2.5

Sector Weights (%)



Top Holdings

Gold - Physical	5.8
Imperial Oil Ltd	1.9
Fomento Economico Mexican SAB de CV	1.4
Danone SA	1.4
Willis Towers Watson plc	1.3
Shell Plc	1.3
Unilever PLC	1.1
Cie Financiere Richemont AG, Zug	1.1
Investor AB publ	1.1
British American Tobacco PLC	1.1
% of Portfolio	17.5

Ten Best Performers

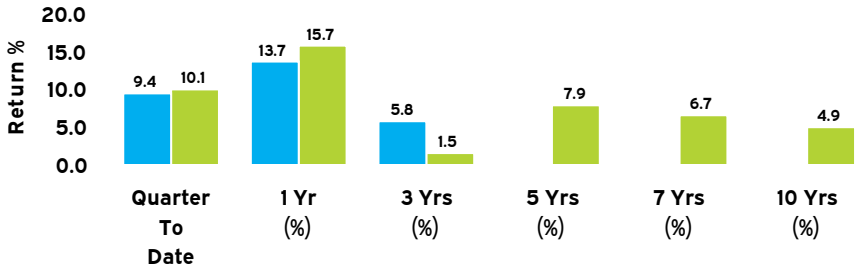
Scholar Education Group
GigaCloud Technology Inc
Zespol Elektrocieplowni Wroclawskich Kogeneracja S.A.,
Snap Inc
Camurus AB
Azure Power Global Limited
Micronics Japan Co Ltd
Lock & Lock Co Ltd
Honda Atlas Cars (Pakistan) Ltd
Hecto Financial Co Ltd

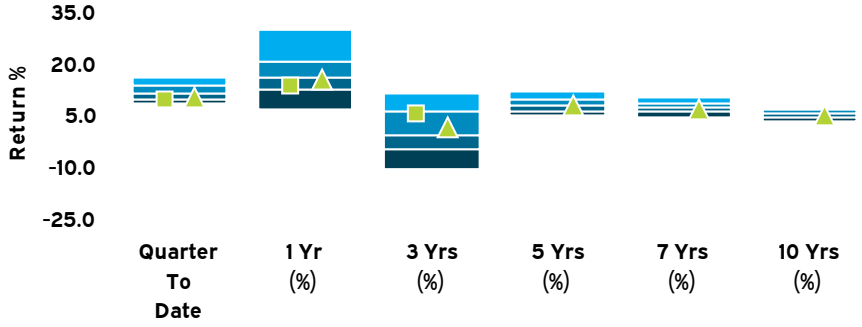
Ten Worst Performers

	Quarterly Return (%)
First Quantum Minerals Ltd	-65.3
Tobii AB	-53.2
Sierra Rutile Holdings Limited	-46.6
Frontier Developments Plc	-38.1
Wismilak Inti Makmur	-37.7
WuXi Biologics (Cayman) Inc	-35.0
Indika Energy TBK	-34.5
Adcorp Holdings	-33.4
Ensign Energy Services Inc	-31.7
Taeyoung Engineering & Construction	-31.7

Acadian ACWI ex U.S. Small Cap Equity | As of December 31, 2023

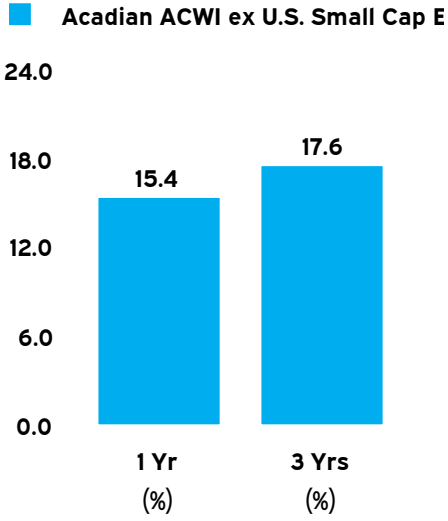
Return Summary



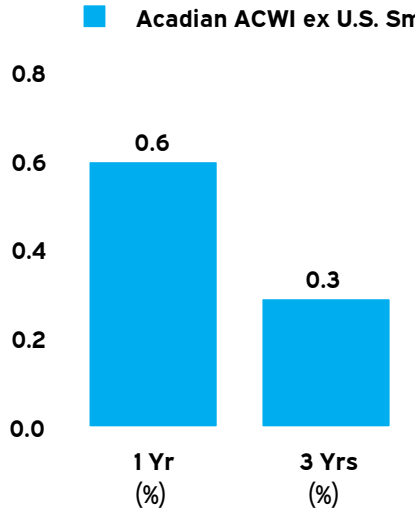


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Acadian ACWI ex U.S. Small Cap Equity	9.4	13.7	5.8	-	-	-
MSCI AC World ex USA Small Cap (Net)	10.1	15.7	1.5	7.9	6.7	4.9
Excess Return	-0.7	-2.0	4.3	-	-	-

Annualized Standard Deviation



Sharpe Ratio



Acadian ACWI ex U.S. Small Cap Equity | As of December 31, 2023

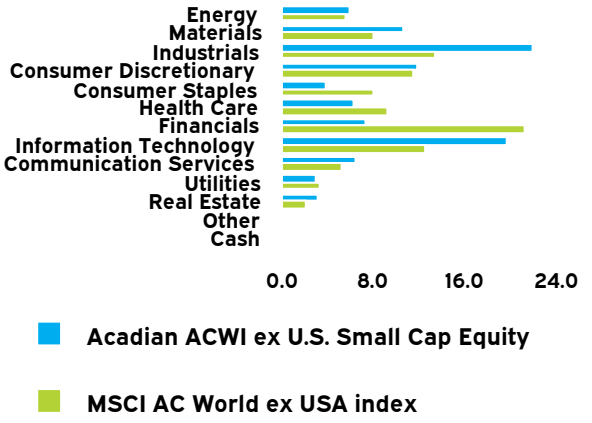
Equity Characteristics vs MSCI AC World ex USA index

	Portfolio	Benchmark
Number of Holdings	1,718	2,312
Wtd. Avg. Mkt. Cap $B	2.4	90.3
Median Mkt. Cap $B	0.5	9.8
P/E Ratio	10.2	13.6
Yield (%)	3.8	3.1
EPS Growth - 5 Yrs. (%)	16.0	10.4
Price to Book	2.1	2.5

Account Information

Account Name	Acadian ACWI ex U.S. Small Cap Equity
Account Structure	Commingled Fund
Inception Date	04/04/2019
Asset Class	International Equity
Benchmark	MSCI AC World ex USA Small Cap (Net)
Peer Group	eV ACWI ex-US Small Cap Equity

Sector Weights (%)



Top Holdings

SCREEN Holdings Co Ltd	1.2
Marks and Spencer Group PLC	1.2
International Games System Co Ltd	1.0
A2A SPA	0.9
MakeMyTrip Ltd	0.9
Boral Ltd Bld	0.9
Chicony Electronics Co Ltd	0.8
WNS (Holdings) Ltd	0.8
Finning International Inc	0.7
Thyssenkrupp AG, Duisburg/Essen	0.7
% of Portfolio	9.1

Ten Best Performers

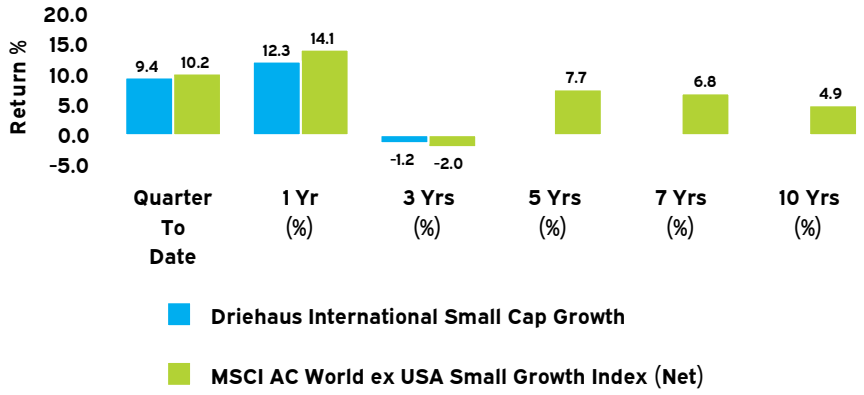
Scholar Education Group
GigaCloud Technology Inc
Zespol Elektrocieplowni Wroclawskich Kogeneracja S.A.,
Camurus AB
Azure Power Global Limited
Micronics Japan Co Ltd
Lock & Lock Co Ltd
Hecto Financial Co Ltd
SCREEN Holdings Co Ltd
Troax Group AB

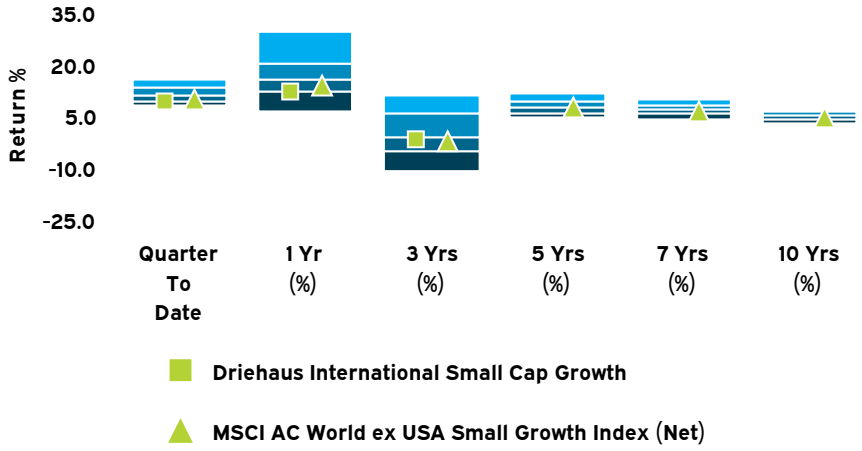
Ten Worst Performers

	Quarterly Return (%)
Tobii AB	-53.2
Sierra Rutile Holdings Limited	-46.6
Frontier Developments Plc	-38.1
Wismilak Inti Makmur	-37.7
Indika Energy TBK	-34.5
Adcorp Holdings	-33.4
Ensign Energy Services Inc	-31.7
Taeyoung Engineering & Construction	-31.7
Indivior PLC	-30.4
XD Inc	-28.0

Driehaus International Small Cap Growth | As of December 31, 2023

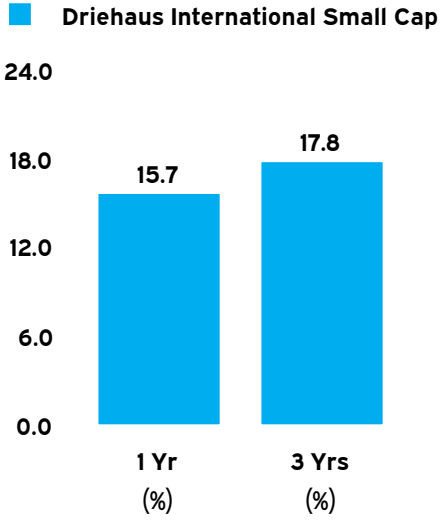
Return Summary



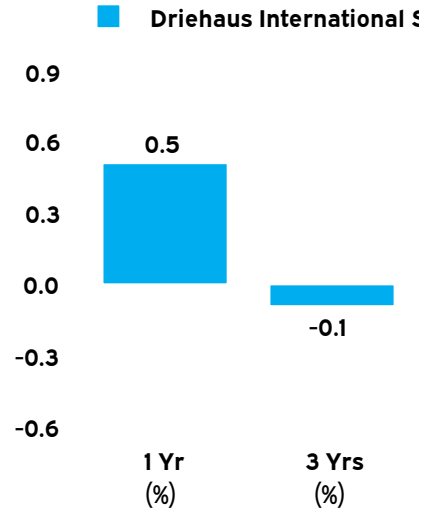


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Driehaus International Small Cap Growth	9.4	12.3	-1.2	-	-	-
MSCI AC World ex USA Small Growth Index (Net)	10.2	14.1	-2.0	7.7	6.8	4.9
Excess Return	-0.8	-1.8	0.8	-	-	-

Annualized Standard Deviation



Sharpe Ratio



Driehaus International Small Cap Growth | As of December 31, 2023

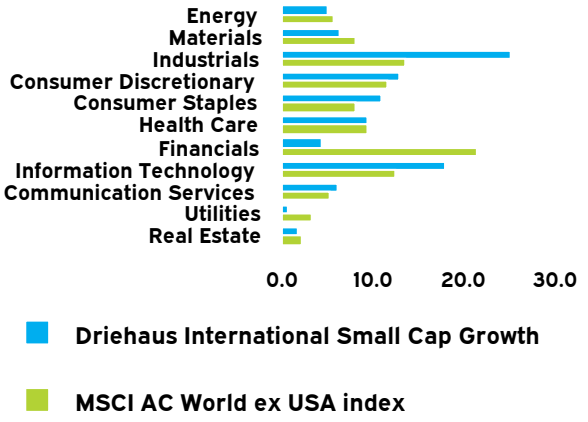
Equity Characteristics vs MSCI AC World ex USA index

	Portfolio	Benchmark
Number of Holdings	113	2,312
Wtd. Avg. Mkt. Cap $B	4.8	90.3
Median Mkt. Cap $B	4.1	9.8
P/E Ratio	16.2	13.6
Yield (%)	1.4	3.1
EPS Growth - 5 Yrs. (%)	10.6	10.4
Price to Book	2.6	2.5

Account Information

Account Name	Driehaus International Small Cap Growth
Account Structure	Commingled Fund
Inception Date	04/25/2019
Asset Class	International Equity
Benchmark	MSCI AC World ex USA Small Growth Index (Net)
Peer Group	eV ACWI ex-US Small Cap Equity

Sector Weights (%)



Top Holdings

Miscellaneous Security	4.8
Fugro NV	2.0
ConvaTec Group PLC	1.9
Glanbia PLC	1.9
Leonardo SPA	1.9
Aixtron SE	1.8
DO & CO AG	1.6
Celestica Inc	1.6
Indra Sistemas SA, Madrid	1.4
Seadrill Ltd	1.4
% of Portfolio	20.3

Ten Best Performers

	Quarterly Return (%)
Alfen N.V.	56.6
JINS HOLDINGS Inc	56.0
Be Semiconductor Industries NV	53.1
HPSP Co Ltd	52.4
Jeol Ltd	47.0
James Hardie Industries Plc	46.4
Rolls Royce Holdings PLC	41.7
Comet Holding AG, Wuennewil-Flamatt	41.0
Mycronic AB	37.1
Lotes Co Ltd	36.7

Ten Worst Performers

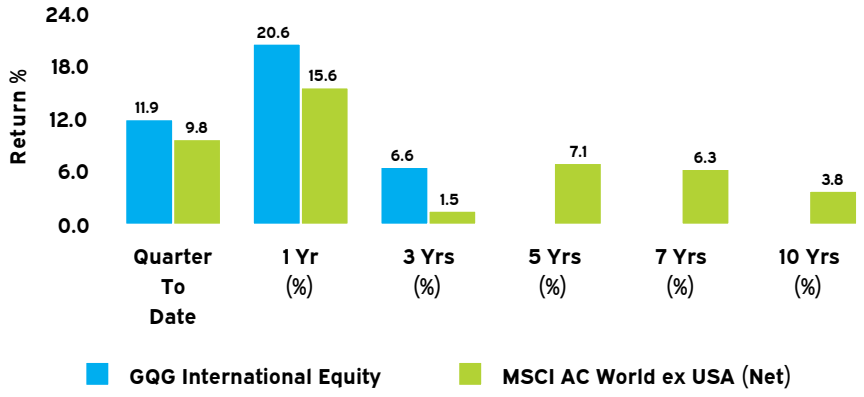
	Quarterly Return (%)
Rohto Pharmaceutical Co Ltd	-25.8
UBI Soft Entertainment SA	-21.6
Syngene International Ltd	-13.0
Sanrio Co Ltd	-12.4
Bumrungrad Hospital Public Co Ltd	-11.6
Capcom Co Ltd	-10.4
Asics Corp	-9.8
CAE Inc.	-7.5
APL Apollo Tubes Ltd	-5.6
Paladin Energy Ltd	-5.3

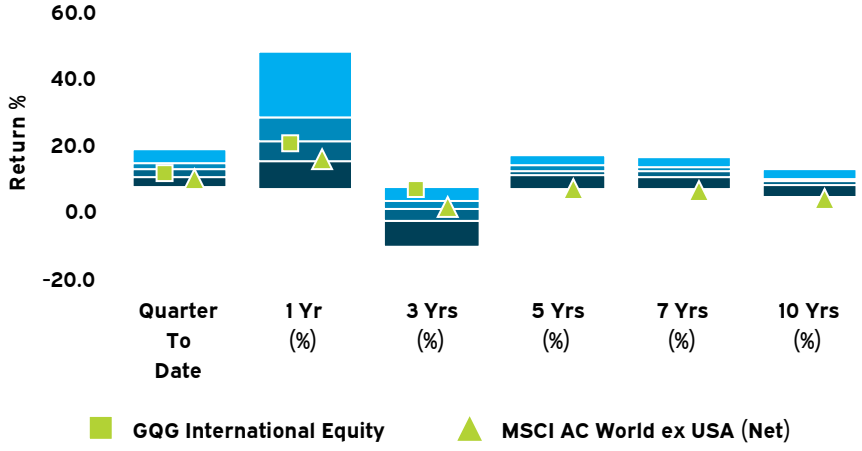
MEKETA

Merced County Employees' Retirement Association

GQG International Equity | As of December 31, 2023

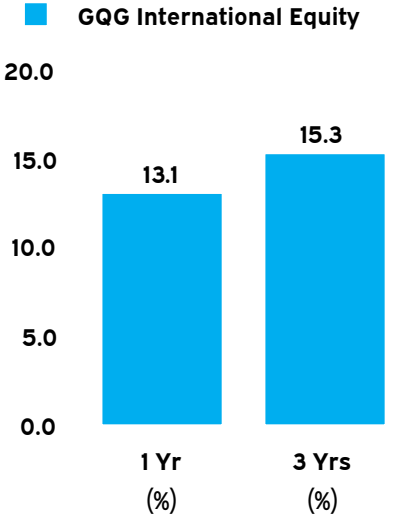
Return Summary



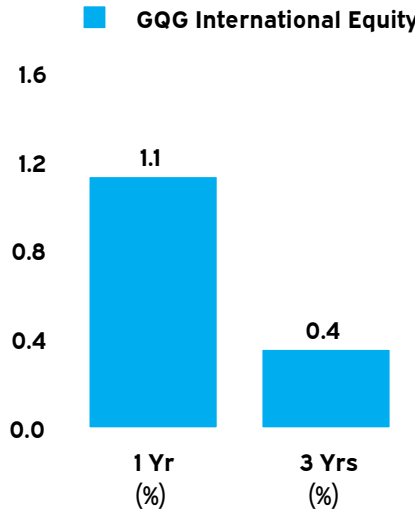


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
GQG International Equity	11.9	20.6	6.6	-	-	-
MSCI AC World ex USA (Net)	9.8	15.6	1.5	7.1	6.3	3.8
Excess Return	2.1	5.0	5.1	-	-	-

Annualized Standard Deviation



Sharpe Ratio



MEKETA

Merced County Employees' Retirement Association

GQG International Equity | As of December 31, 2023

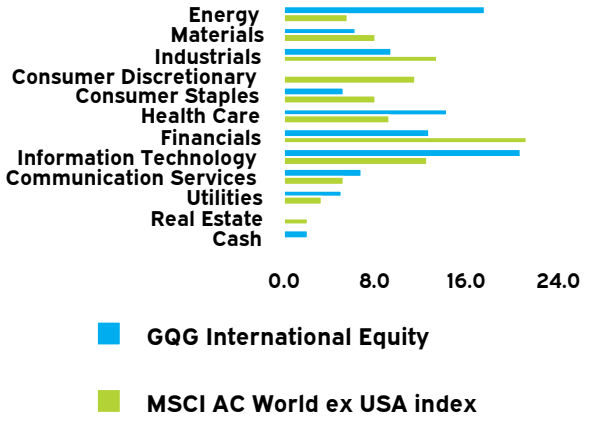
Equity Characteristics vs MSCI AC World ex USA index

	Portfolio	Benchmark
Number of Holdings	61	2,312
Wtd. Avg. Mkt. Cap $B	244.8	90.3
Median Mkt. Cap $B	73.5	9.8
P/E Ratio	15.5	13.6
Yield (%)	2.9	3.1
EPS Growth - 5 Yrs. (%)	17.2	10.4
Price to Book	3.5	2.5

Account Information

Account Name	GQG International Equity
Account Structure	Commingled Fund
Inception Date	12/01/2019
Asset Class	International Equity
Benchmark	MSCI AC World ex USA (Net)
Peer Group	eV Global Growth Equity

Sector Weights (%)



Top Holdings

Novo Nordisk A/S	6.9
Astrazeneca PLC	5.3
TotalEnergies SE	5.2
NVIDIA Corporation	5.0
Glencore Plc	4.7
ASML Holding NV	3.0
Canadian Natural Resources Ltd	2.5
Broadcom Inc	2.4
Icici Bank Ltd	2.4
ASML Holding NV	2.2
% of Portfolio	39.6

Ten Best Performers

	Quarterly Return (%)
Adani Green Energy Limited	61.4
Shin-Etsu Chemical Co Ltd	44.2
Advanced Micro Devices Inc	43.4
Shopify Inc	42.8
Rolls Royce Holdings PLC	41.7
Arm Holdings plc	40.4
Adani Power Ltd	38.8
Broadcom Inc	35.0
GMR Airports Infrastructure Limited	35.0
Tokyo Electron Ltd	30.8

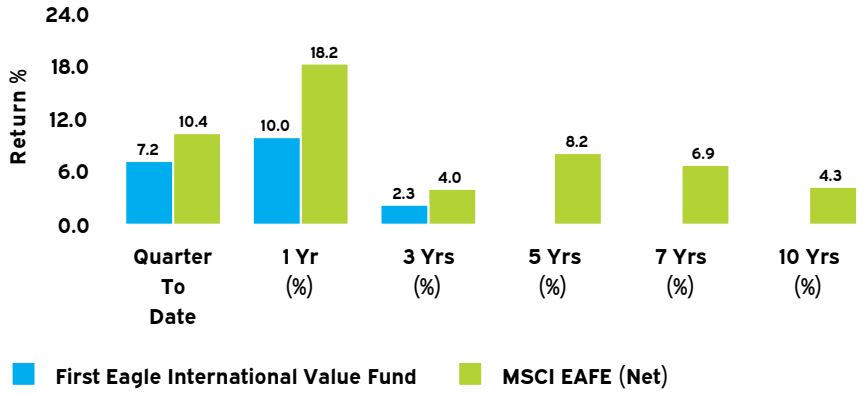
Ten Worst Performers

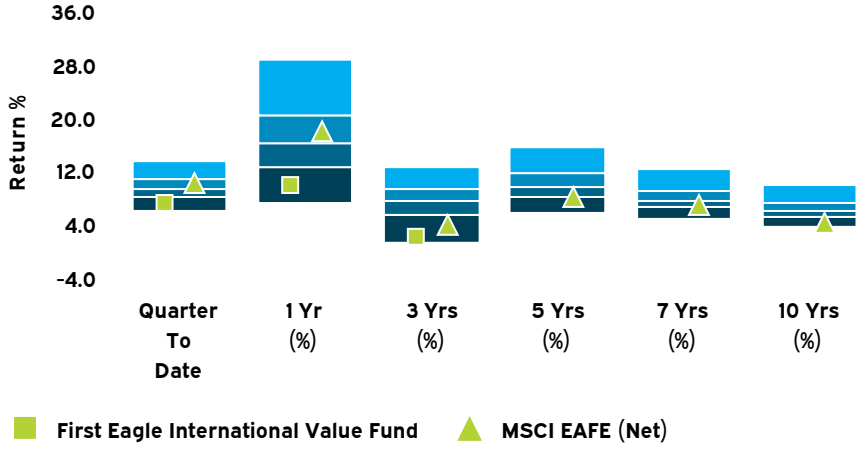
	Quarterly Return (%)
Schlumberger Ltd	-10.3
Aon plc	-10.1
Tourmaline Oil Corp	-9.0
IDFC First Bank Ltd	-7.1
Astrazeneca PLC	-0.3
International Holding Co PJSC	-0.3
Canadian Natural Resources Ltd	2.5
Shell Plc	3.0
TotalEnergies SE	3.1
Novartis AG	3.7

Merced County Employees' Retirement Association

First Eagle International Value Fund | As of December 31, 2023

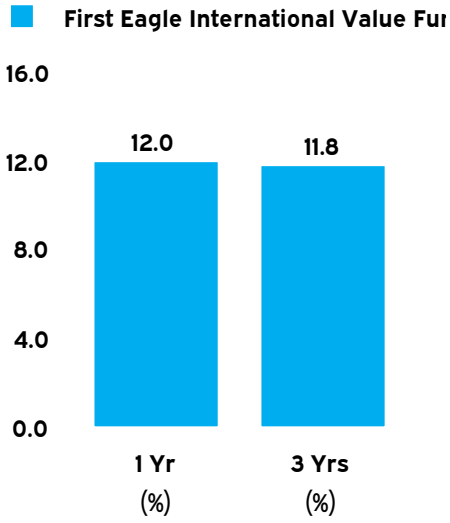
Return Summary



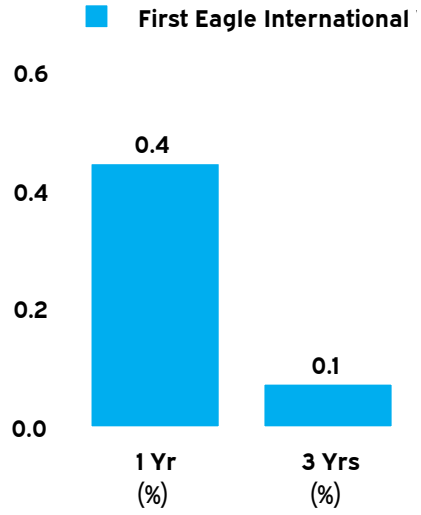


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
First Eagle International Value Fund	7.2	10.0	2.3	-	-	-
MSCI EAFE (Net)	10.4	18.2	4.0	8.2	6.9	4.3
Excess Return	-3.2	-8.2	-1.7	-	-	-

Annualized Standard Deviation



Sharpe Ratio



First Eagle International Value Fund | As of December 31, 2023

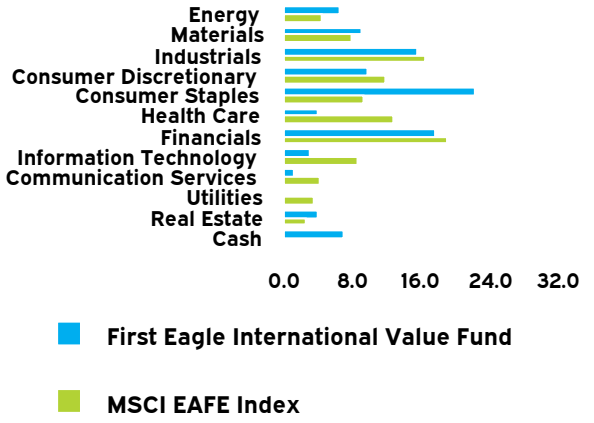
Equity Characteristics vs MSCI EAFE Index

	Portfolio	Benchmark
Number of Holdings	106	783
Wtd. Avg. Mkt. Cap $B	38.7	88.5
Median Mkt. Cap $B	16.2	13.4
P/E Ratio	13.2	13.7
Yield (%)	3.0	3.2
EPS Growth - 5 Yrs. (%)	7.5	9.9
Price to Book	1.8	2.6

Account Information

Account Name	First Eagle International Value Fund
Account Structure	Commingled Fund
Inception Date	12/01/2019
Asset Class	International Equity
Benchmark	MSCI EAFE (Net)
Peer Group	eV Global Value Equity

Sector Weights (%)



Top Holdings

Gold - Physical	10.5
Imperial Oil Ltd	3.5
Fomento Economico Mexican SAB de CV	2.5
Danone SA	2.5
Willis Towers Watson plc	2.4
Shell Plc	2.3
Unilever PLC	2.0
Cie Financiere Richemont AG, Zug	1.9
Investor AB publ	1.9
British American Tobacco PLC	1.9
% of Portfolio	31.4

Ten Best Performers

	Quarterly Return (%)
Cia Energetica De Brasilia Ceb	41.2
LE Lundbergforetagen AB	29.3
Nihon Kohden Corp	28.0
Industrias Penoles S.A.B. de C.V.	26.3
Itausa S A	26.0
Barrick Gold Corp	25.0
Schindler Holding AG, Hergiswil	24.9
Industrivaerden AB	22.6
Wheaton Precious Metals Corp	22.1
Grupo Mexico S.A.B. de C.V.	21.9

Ten Worst Performers

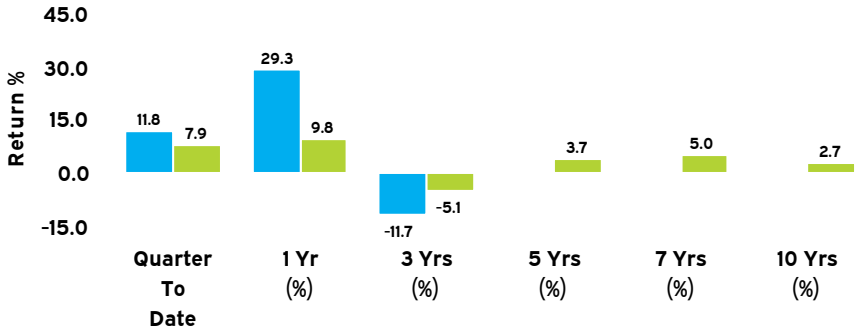
	Quarterly Return (%)
Franco-Nevada Corp	-16.7
AG Anadolu Grubu Holding Anonim Sirketi	-13.9
Pilot Corp	-12.3
Jardine Matheson Holdings Ltd	-11.2
Alibaba Group Holding Ltd	-10.2
Nong Shim Co Ltd	-9.8
Daiichikosho Co Ltd	-9.0
Great Eagle Holdings Ltd	-8.5
Nutrien Ltd	-7.9
Sanofi	-7.7

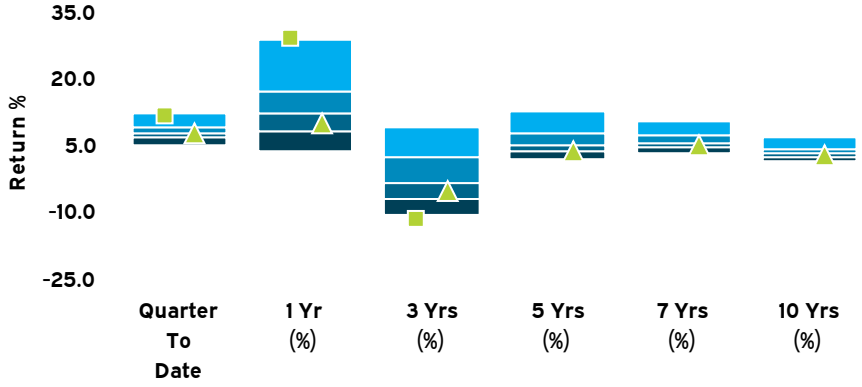
MEKETA

Merced County Employees' Retirement Association

Artisan Developing World TR | As of December 31, 2023

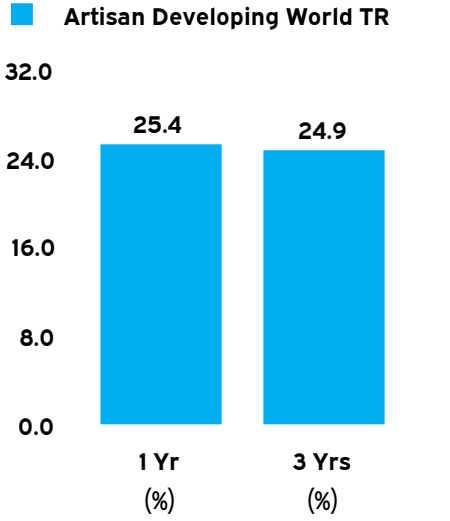
Return Summary



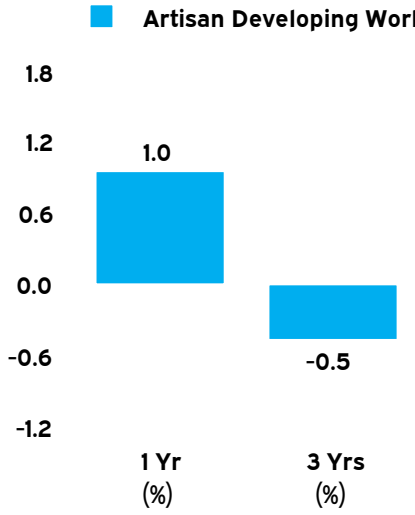


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Artisan Developing World TR	11.8	29.3	-11.7	-	-	-
MSCI Emerging Markets (Net)	7.9	9.8	-5.1	3.7	5.0	2.7
Excess Return	3.9	19.5	-6.6	-	-	-

Annualized Standard Deviation



Sharpe Ratio



Artisan Developing World TR | As of December 31, 2023

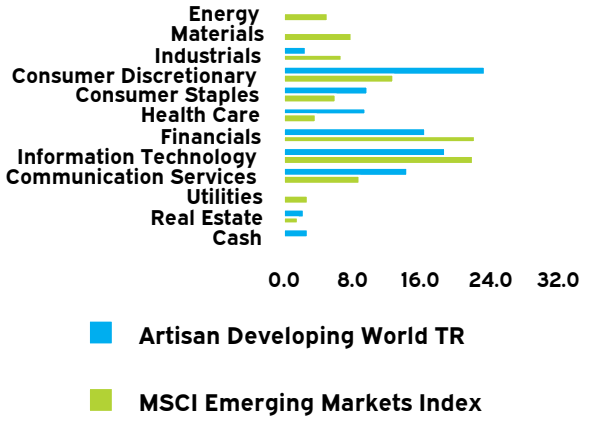
Equity Characteristics vs MSCI Emerging Markets Index

	Portfolio	Benchmark
Number of Holdings	44	1,441
Wtd. Avg. Mkt. Cap $B	168.5	103.8
Median Mkt. Cap $B	49.0	7.0
P/E Ratio	36.5	12.9
Yield (%)	0.5	2.8
EPS Growth - 5 Yrs. (%)	36.2	12.3
Price to Book	5.9	2.5

Account Information

Account Name	Artisan Developing World TR
Account Structure	Commingled Fund
Inception Date	12/01/2019
Asset Class	International Equity
Benchmark	MSCI Emerging Markets (Net)
Peer Group	eV Emg Mkts Equity

Sector Weights (%)



Top Holdings

MercadoLibre Inc	5.6
NVIDIA Corporation	4.8
Visa Inc	4.8
Sea Limited	4.8
MakeMyTrip Ltd	4.7
Airbnb Inc	4.5
Adyen N.V	4.2
CrowdStrike Holdings Inc	3.6
Nu Holdings Ltd	3.2
Meituan	3.2
% of Portfolio	43.4

Ten Best Performers

	Quarterly Return (%)
Snap Inc	90.0
Adyen N.V	72.5
CrowdStrike Holdings Inc	52.5
Datadog Inc	33.3
Unity Software Inc	30.3
Snowflake Inc	30.3
Netflix Inc	28.9
ASML Holding NV	28.9
MercadoLibre Inc	23.9
MakeMyTrip Ltd	15.9

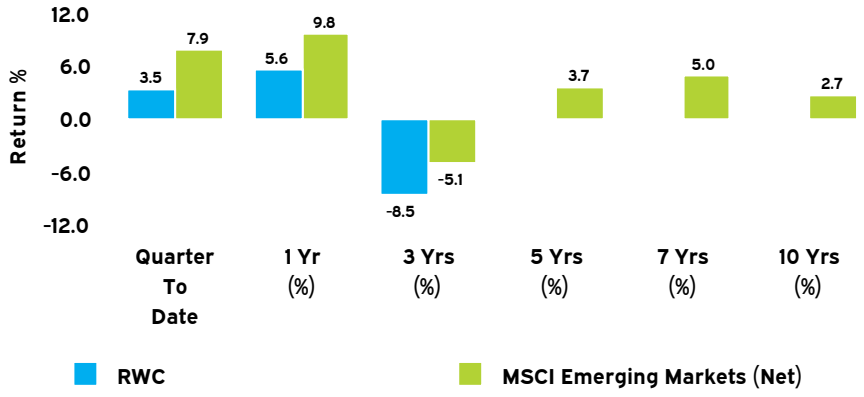
Ten Worst Performers

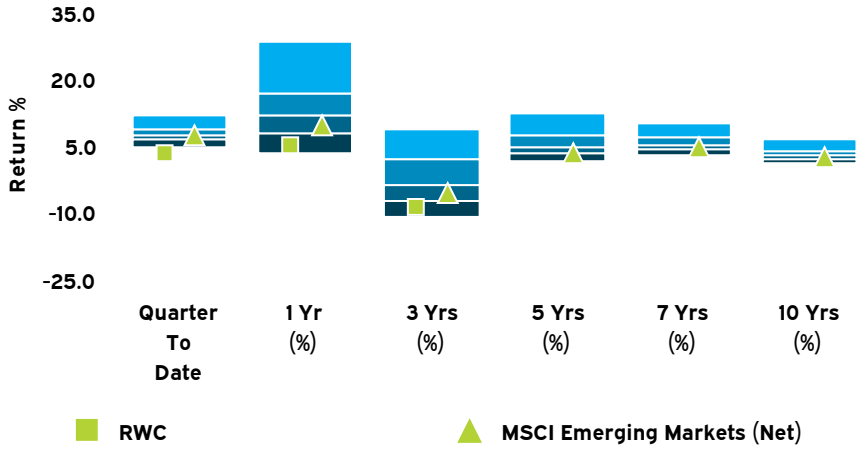
	Quarterly Return (%)
WuXi Biologics (Cayman) Inc	-35.0
Meituan	-28.3
Bilibili Inc	-11.6
Alibaba Group Holding Ltd	-9.4
Sea Limited	-7.8
Veeva Systems Inc	-5.4
Grab Holdings Limited	-4.8
Tencent Holdings LTD	-3.8
JD Health International Inc	-3.4
Airbnb Inc	-0.8

Merced County Employees' Retirement Association

RWC | As of December 31, 2023

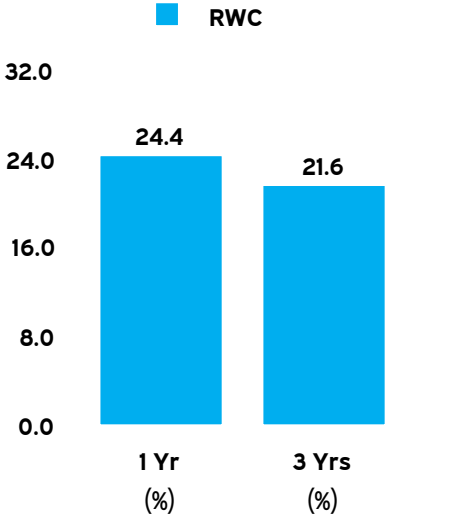
Return Summary



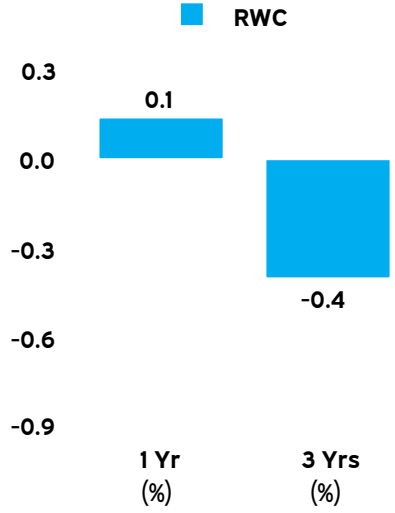


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
RWC	3.5	5.6	-8.5	-	-	-
MSCI Emerging Markets (Net)	7.9	9.8	-5.1	3.7	5.0	2.7
Excess Return	-4.4	-4.2	-3.4	-	-	-

Annualized Standard Deviation



Sharpe Ratio



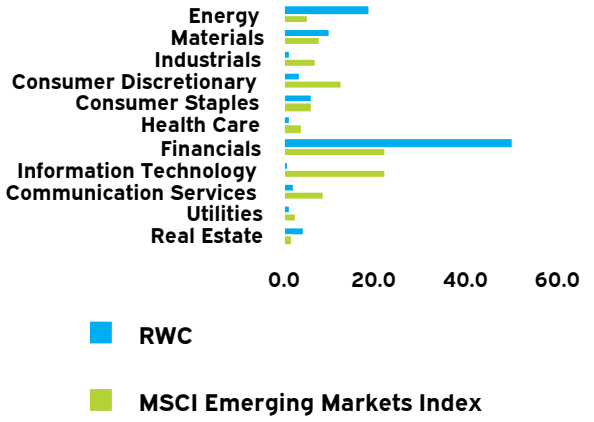
Equity Characteristics vs MSCI Emerging Markets Index

	Portfolio	Benchmark
Number of Holdings	56	1,441
Wtd. Avg. Mkt. Cap $B	1.9	103.8
Median Mkt. Cap $B	0.8	7.0
P/E Ratio	5.6	12.9
Yield (%)	4.6	2.8
EPS Growth - 5 Yrs. (%)	14.1	12.3
Price to Book	1.9	2.5

Account Information

Account Name	RWC
Account Structure	Commingled Fund
Inception Date	12/01/2019
Asset Class	International Equity
Benchmark	MSCI Emerging Markets (Net)
Peer Group	eV Emg Mkts Equity

Sector Weights (%)



Top Holdings

Savannah Energy Plc	5.6
Nova Ljubljanska Banka d.d	4.0
Seplat Energy Plc	3.9
TBC Bank Group PLC	3.7
Georgia Capital Plc	3.6
Addiko Bank AG	3.5
Military Commercial Joint Stock Bank	3.5
Halyk Bank of Kazakhstan Joint Stock Company	3.4
Guaranty Trust Bank PLC	3.2
Kazatomprom JSC NAC	3.1
% of Portfolio	37.5

Ten Best Performers

Honda Atlas Cars (Pakistan) Ltd
Meezan Bank Ltd
Telecom Argentina SA
Lucky Cement Ltd
Ypf Sociedad Anonima Yacimientos Petroliferos Fiscales
United Bank Limited
Grupo Financiero Galicia Sa, Buenos Aires
NGEX Minerals Ltd
Sphera Franchise Group S.A.
Nova Ljubljanska Banka d.d

Ten Worst Performers

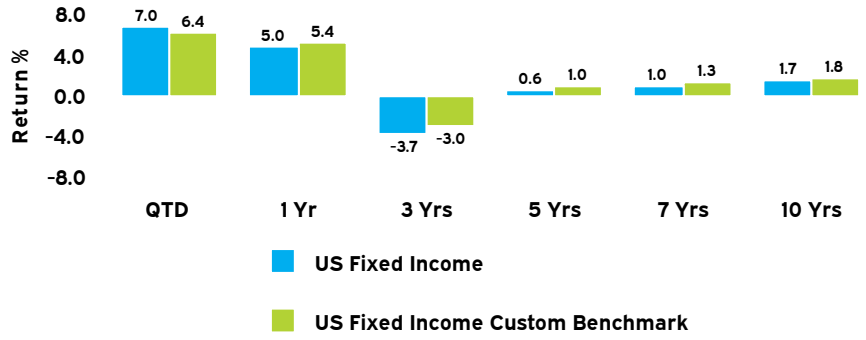
	Quarterly Return (%)
First Quantum Minerals Ltd	-65.3
Nigerian Breweries PLC	-21.6
SolGold PLC	-20.6
East African Breweries Ltd	-17.9
Ceylon Cold Stores Ltd	-13.6
Masan Group Corp	-12.0
Equity Group Holdings Ltd	-10.6
Vincom Retail Co Ltd	-10.6
Vietnam Dairy Product Co	-8.1
Kazatomprom JSC NAC	-7.4

MEKETA

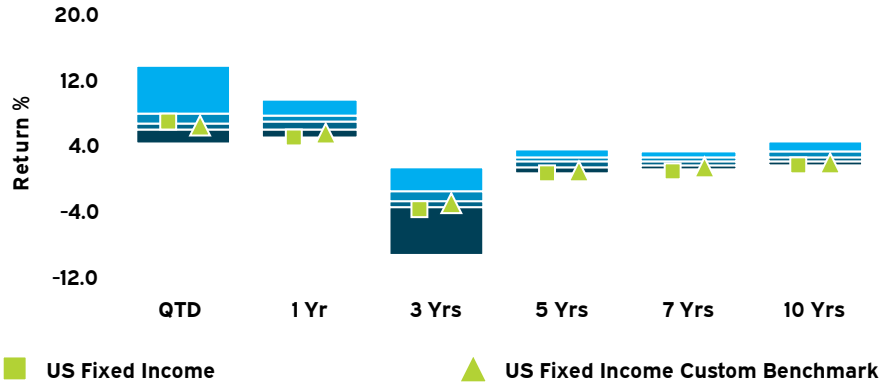
Merced County Employees' Retirement Association

US Fixed Income | As of December 31, 2023

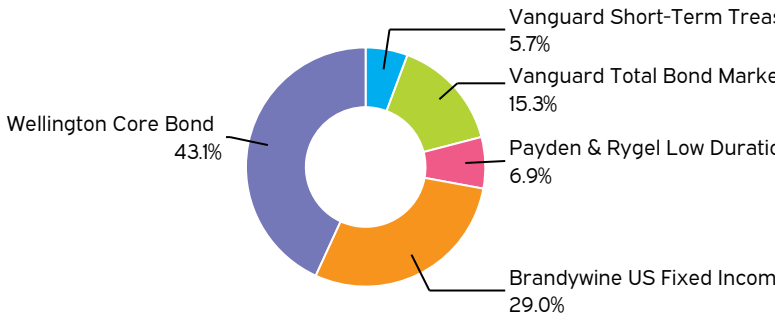
Return Summary



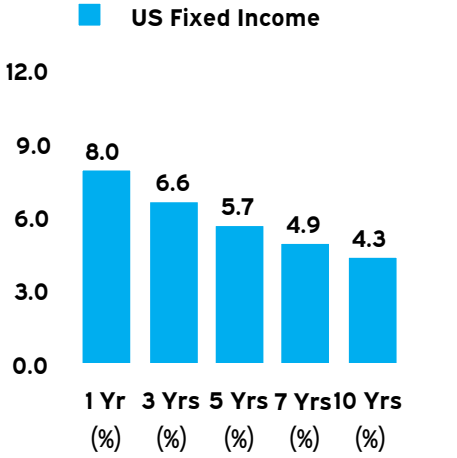
	QTD (%)	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
US Fixed Income	7.0	5.0	-3.7	0.6	1.0	1.7
US Fixed Income Custom Benchmark	6.4	5.4	-3.0	1.0	1.3	1.8
Excess Return	0.6	-0.4	-0.7	-0.4	-0.3	-0.1



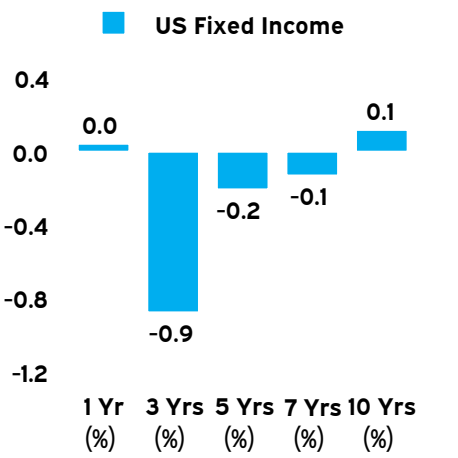
Current Allocation



Annualized Standard Deviation



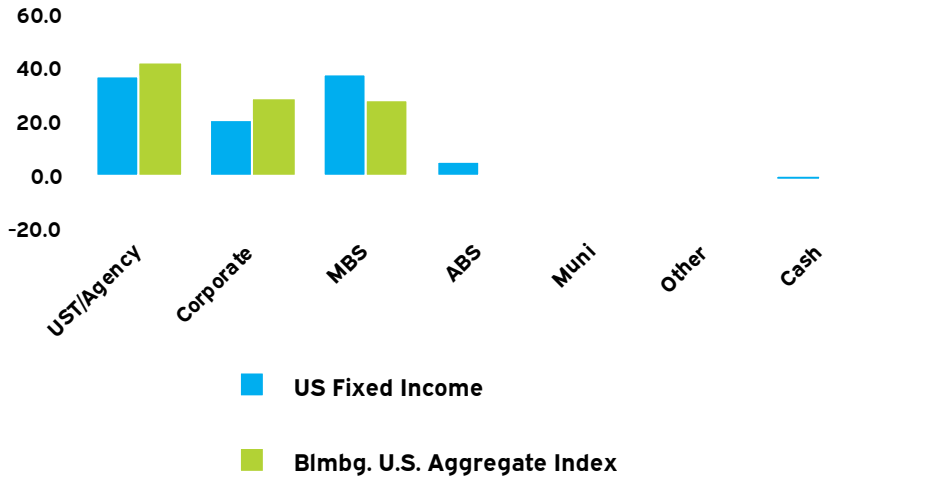
Sharpe Ratio



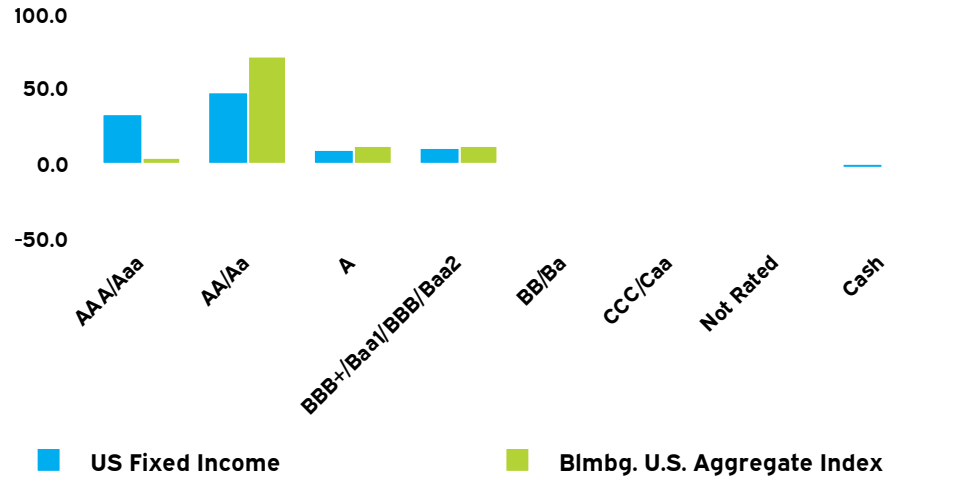
US Fixed Income Portfolio Characteristics

	Portfolio	Benchmark
Yield To Maturity (%)	4.9	4.5
Effective Duration	7.3	-
Avg. Quality	AA	AA

Sector Distribution (%)

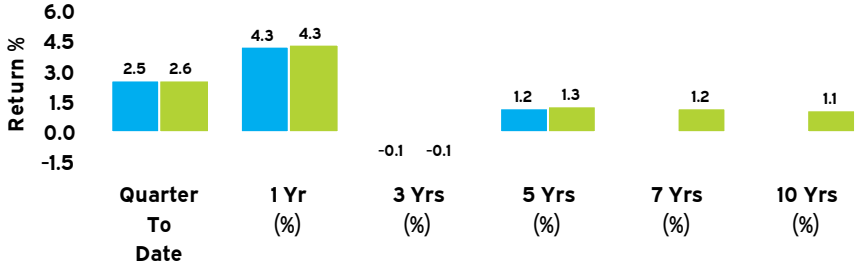


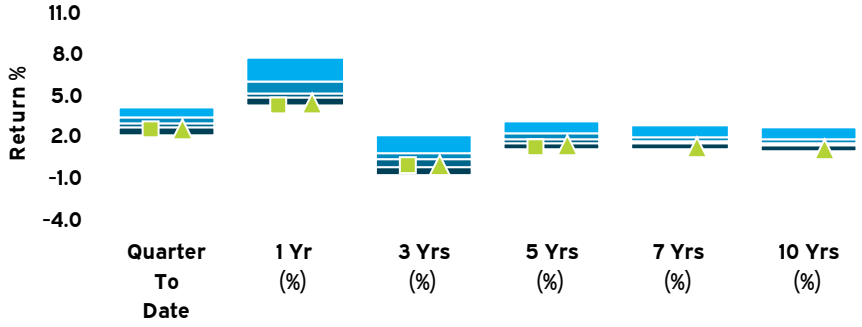
Credit Quality Distribution (%)



Vanguard Short-Term Treasury Index Fund | As of December 31, 2023

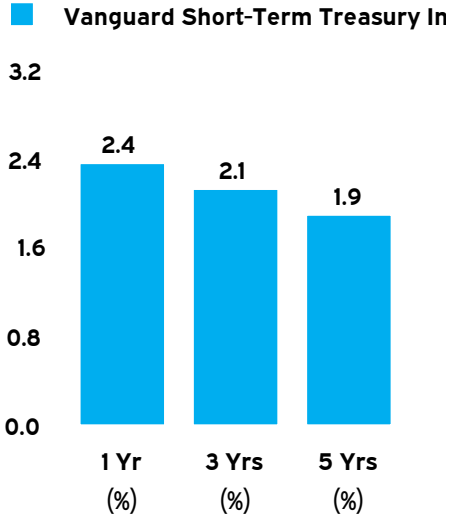
Return Summary



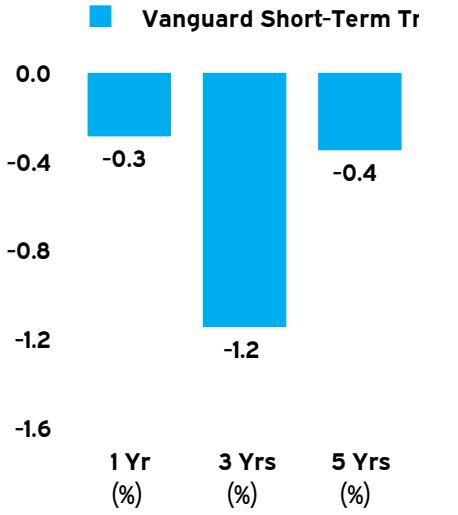


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Vanguard Short-Term Treasury Index Fund	2.5	4.3	-0.1	1.2	-	-
Blmbg. 1-3 Govt	2.6	4.3	-0.1	1.3	1.2	1.1
Excess Return	-0.1	0.0	0.0	-0.1	-	-

Annualized Standard Deviation



Sharpe Ratio



Vanguard Short-term TIPS | As of December 31, 2023

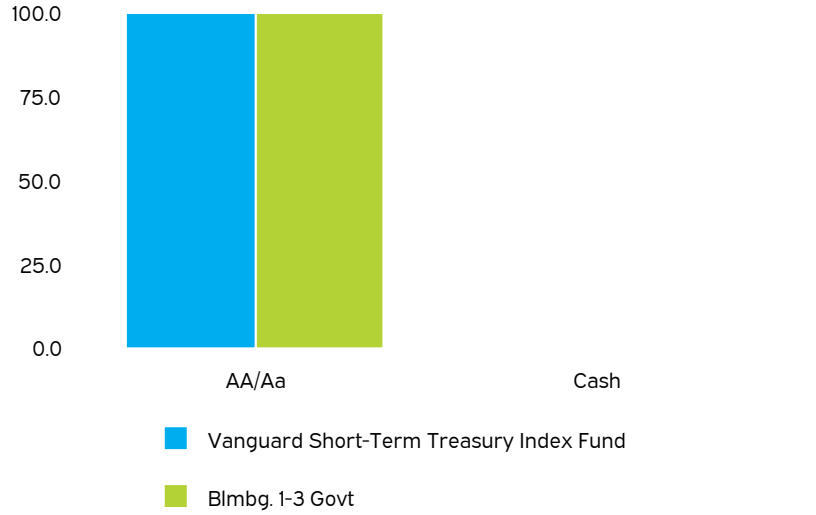
Account Information

Account Name	Vanguard Short-Term Treasury Index Fund
Inception Date	02/26/2018
Account Structure	Mutual Fund
Asset Class	US Fixed Income
Benchmark	Blmbg. 1-3 Govt

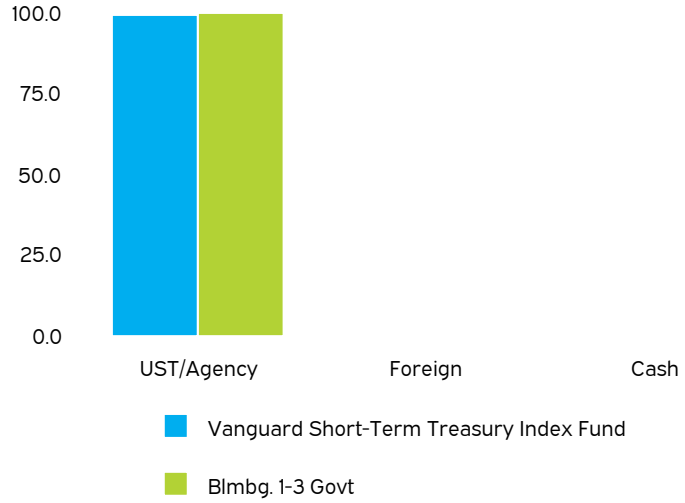
Fixed Income Characteristics

	Q4 -23	Q3 -23
	Vanguard Short-Term Treasury Index Fund	Vanguard Short-Term Treasury Index Fu
Yield To Maturity	4.76	4.91
Average Duration	1.89	1.89
Average Quality	AA	AA
Weight Average Maturity	2.00	2.00

Credit Quality Allocation

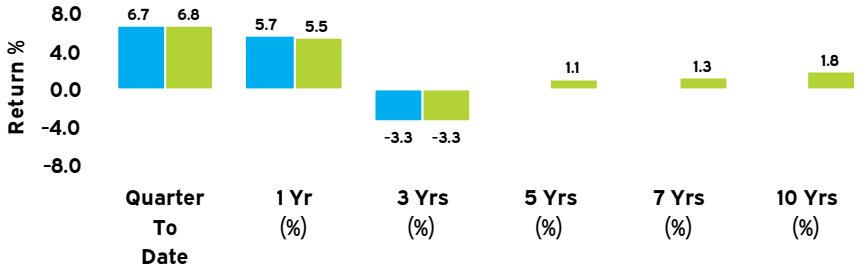


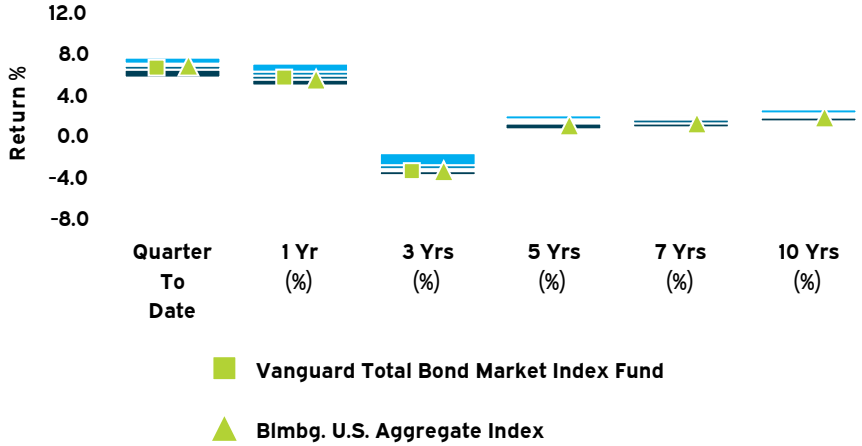
Sector Distribution



Vanguard Total Bond Market Index Fund | As of December 31, 2023

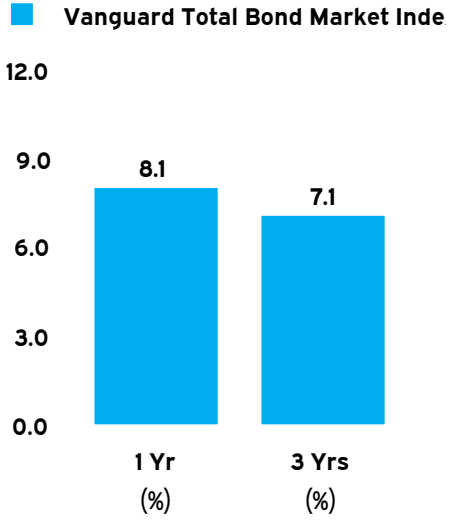
Return Summary



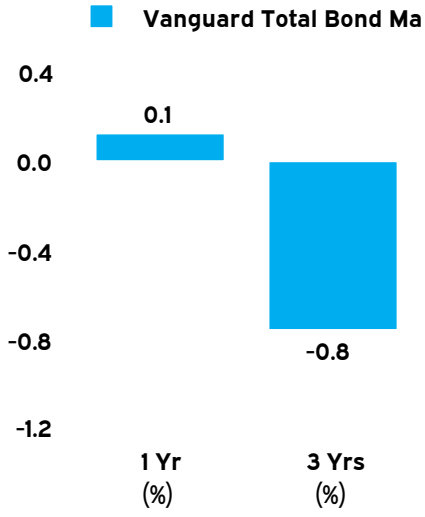


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Vanguard Total Bond Market Index Fund	6.7	5.7	-3.3	-	-	-
Blmbg. U.S. Aggregate Index	6.8	5.5	-3.3	1.1	1.3	1.8
Excess Return	-0.1	0.2	0.0	-	-	-

Annualized Standard Deviation



Sharpe Ratio

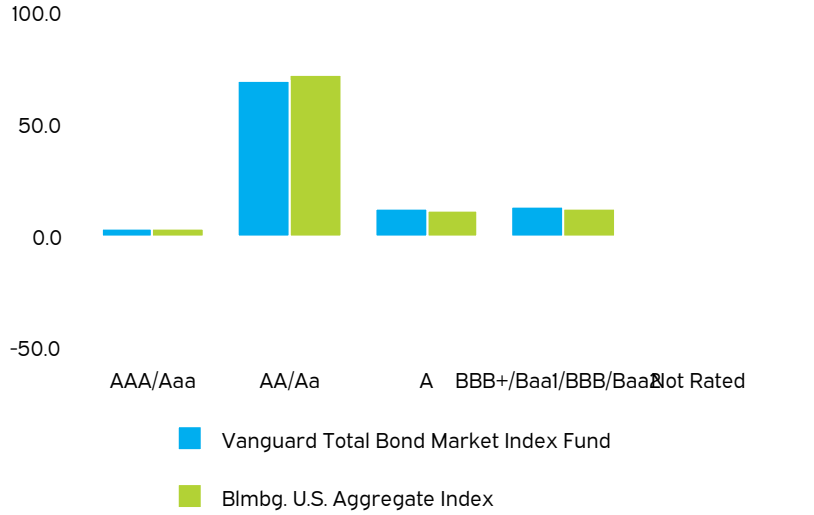


Vanguard Total Bond Market Index Fund | As of December 31, 2023

Account Information

Account Name	Vanguard Total Bond Market Index Fund
Inception Date	04/12/2019
Account Structure	Mutual Fund
Asset Class	US Fixed Income
Benchmark	Blmbg. U.S. Aggregate Index

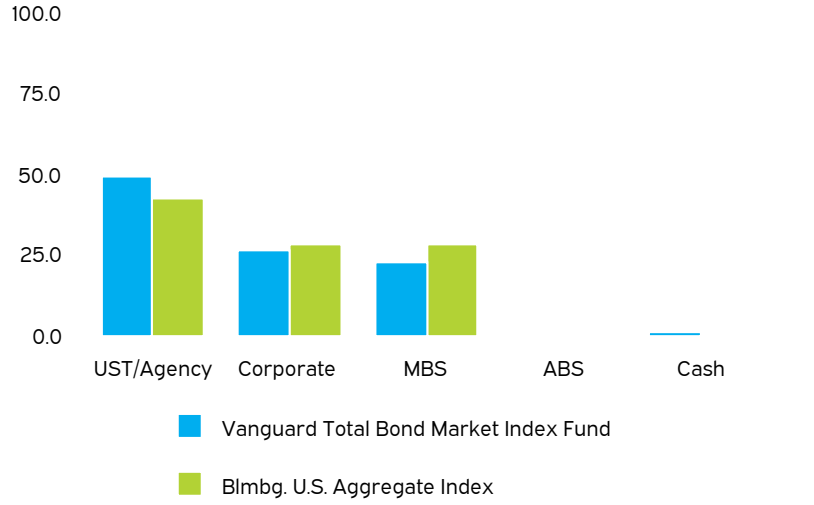
Credit Quality Allocation



Fixed Income Characteristics

	Q4 -23	
	Vanguard Total Bond Market Index Fund	Blmbg. U.S. Aggregate In
Yield To Maturity	5.00	4.53
Average Duration	6.30	6.24
Average Quality	AA	AA
Weight Average Maturity	8.70	8.46

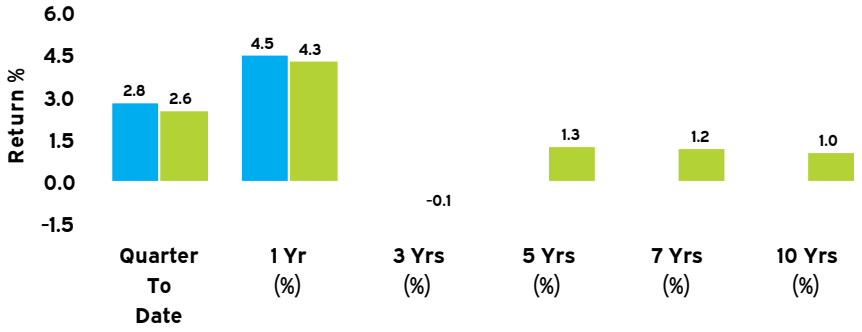
Sector Distribution

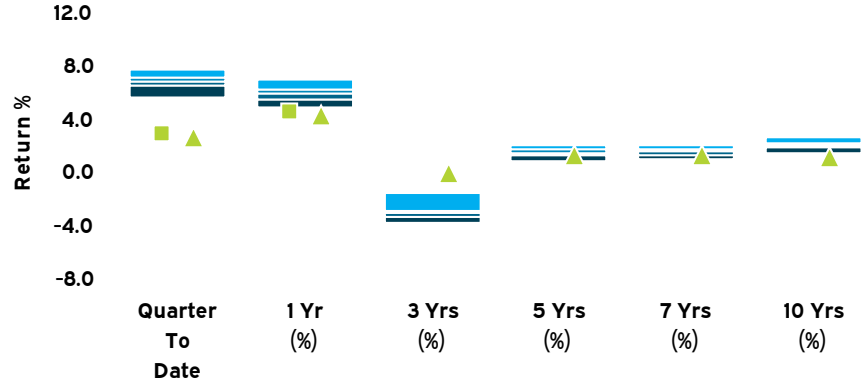


Merced County Employees' Retirement Association

Payden & Rygel Low Duration Fund | As of December 31, 2023

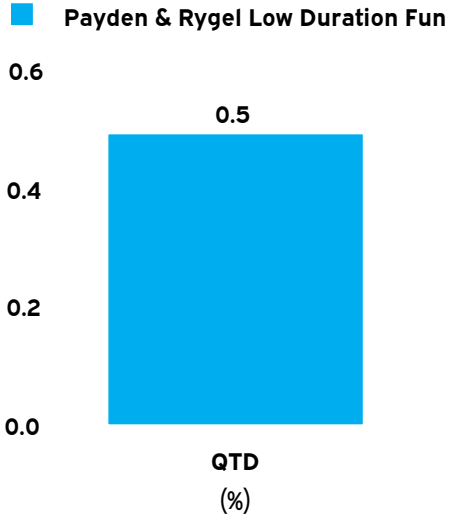
Return Summary



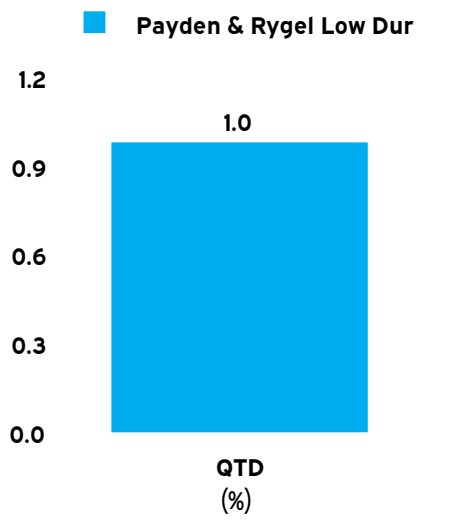


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Payden & Rygel Low Duration Fund	2.8	4.5	-	-	-	-
Blmbg. U.S. Treasury: 1-3 Year	2.6	4.3	-0.1	1.3	1.2	1.0
Excess Return	0.2	0.2	-	-	-	-

Annualized Standard Deviation



Sharpe Ratio



Payden & Rygel Low Duration Fund | As of December 31, 2023

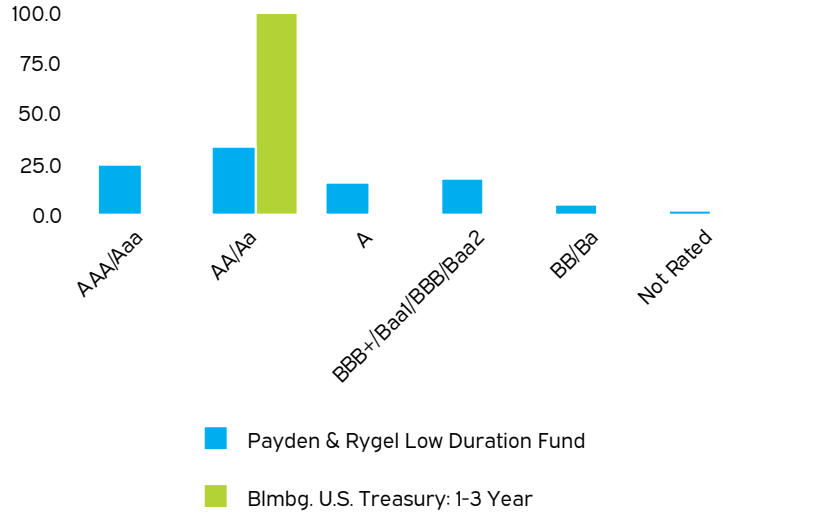
Account Information

Account Name	Payden & Rygel Low Duration Fund
Inception Date	11/01/2022
Account Structure	Mutual Fund
Asset Class	US Fixed Income
Benchmark	Blmbg. U.S. Treasury: 1-3 Year

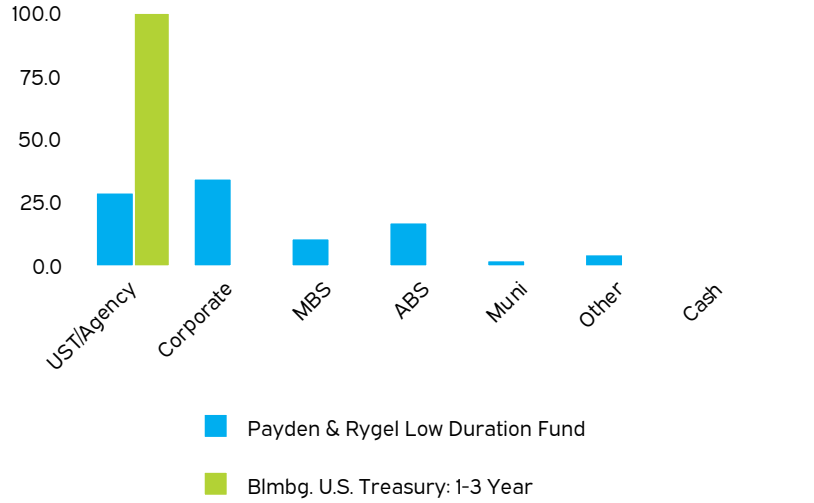
Fixed Income Characteristics

	Q4 -23	
	Payden & Rygel Low Duration Fund	Blmbg. U.S. Treasury: 1-3 Yea
Yield To Maturity	5.66	4.33
Average Duration	1.84	1.84
Average Quality	AA	AA
Weight Average Maturity	2.10	1.97

Credit Quality Allocation



Sector Distribution

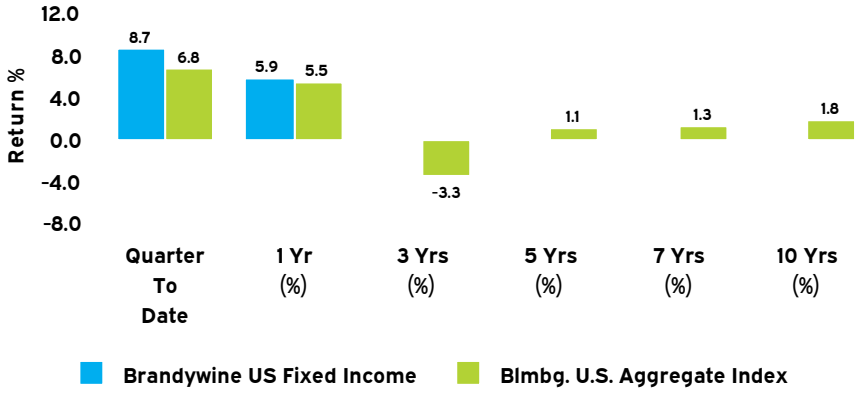


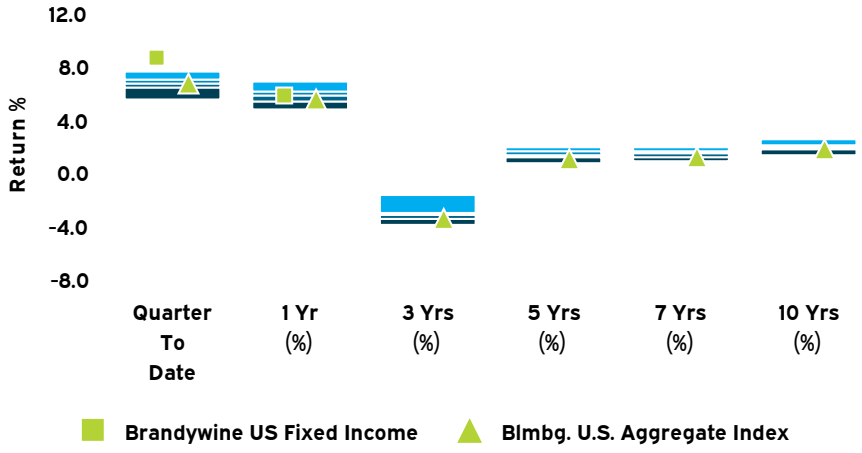
MEKETA

Merced County Employees' Retirement Association

Brandywine US Fixed Income | As of December 31, 2023

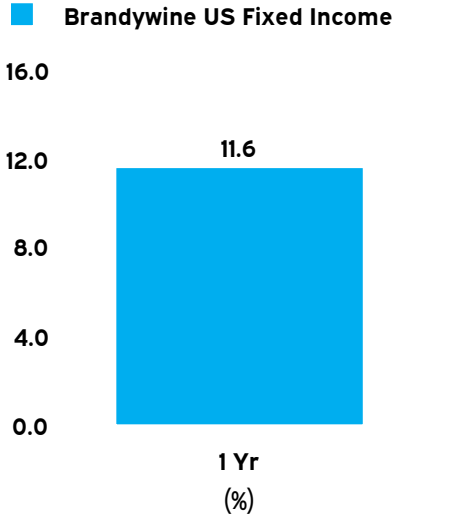
Return Summary



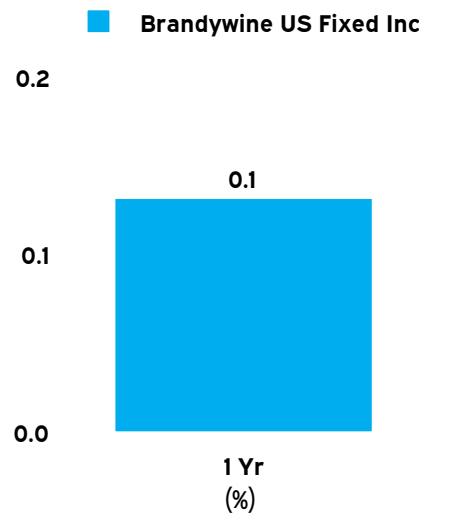


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Brandywine US Fixed Income	8.7	5.9	-	-	-	-
Blmbg. U.S. Aggregate Index	6.8	5.5	-3.3	1.1	1.3	1.8
Excess Return	1.9	0.4	-	-	-	-

Annualized Standard Deviation



Sharpe Ratio



Brandywine US Fixed Income | As of December 31, 2023

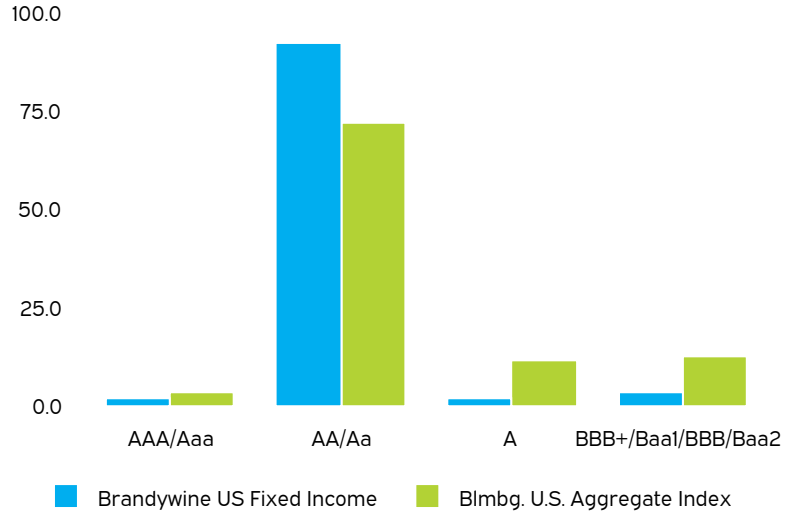
Account Information

Account Name	Brandywine US Fixed Income
Inception Date	11/01/2022
Account Structure	Mutual Fund
Asset Class	US Fixed Income
Benchmark	Blmbg. U.S. Aggregate Index

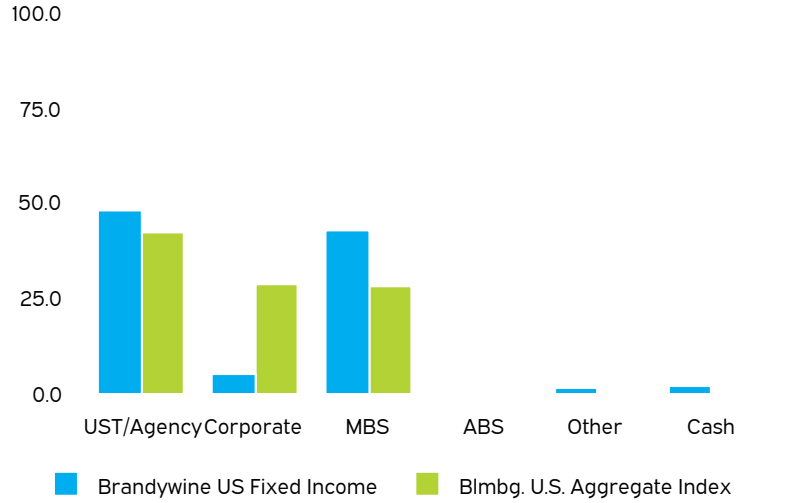
Fixed Income Characteristics

	Q4 -23	
	Brandywine US Fixed Income	Blmbg. U.S. Aggregate Inde
Yield To Maturity	4.55	4.53
Average Duration	9.01	6.24
Average Quality	AA	AA
Weight Average Maturity	19.95	8.46

Credit Quality Allocation



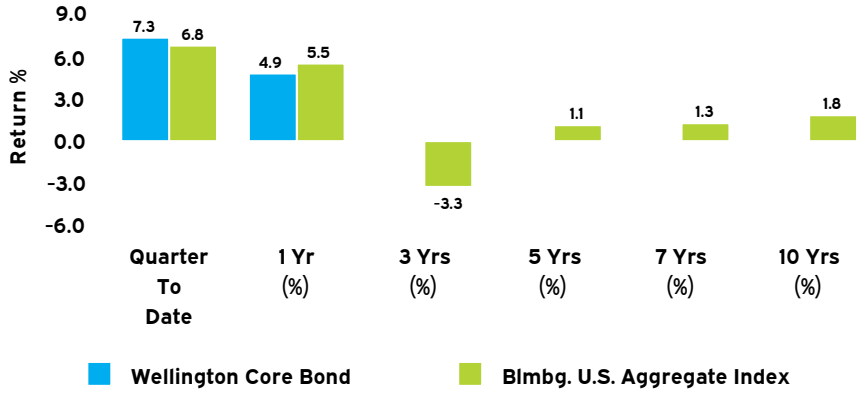
Sector Distribution

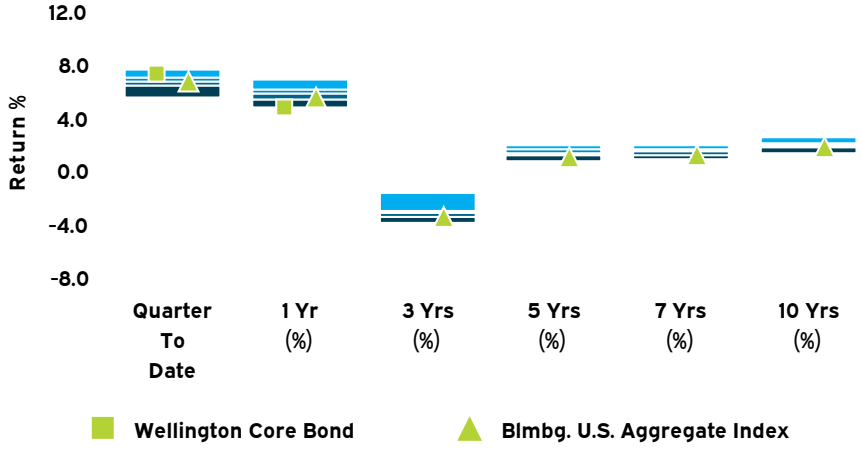


Merced County Employees' Retirement Association

Wellington Core Bond | As of December 31, 2023

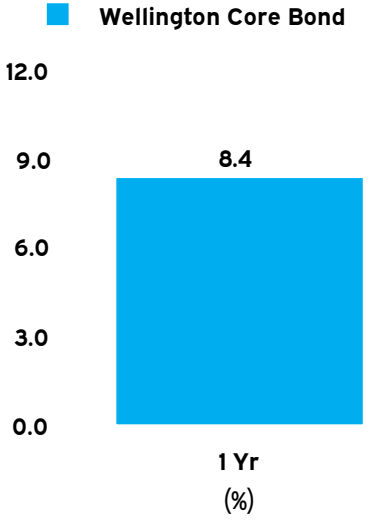
Return Summary



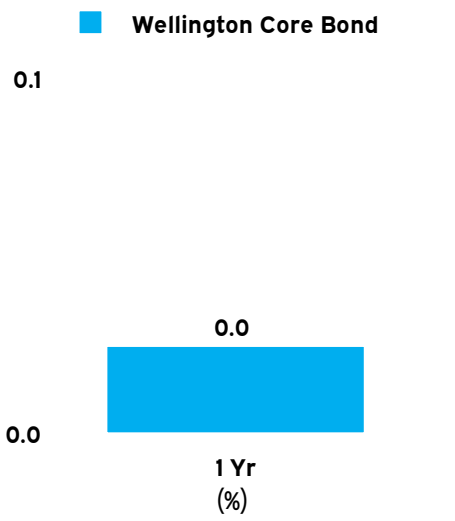


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Wellington Core Bond	7.3	4.9	-	-	-	-
Blmbg. U.S. Aggregate Index	6.8	5.5	-3.3	1.1	1.3	1.8
Excess Return	0.5	-0.6	-	-	-	-

Annualized Standard Deviation



Sharpe Ratio

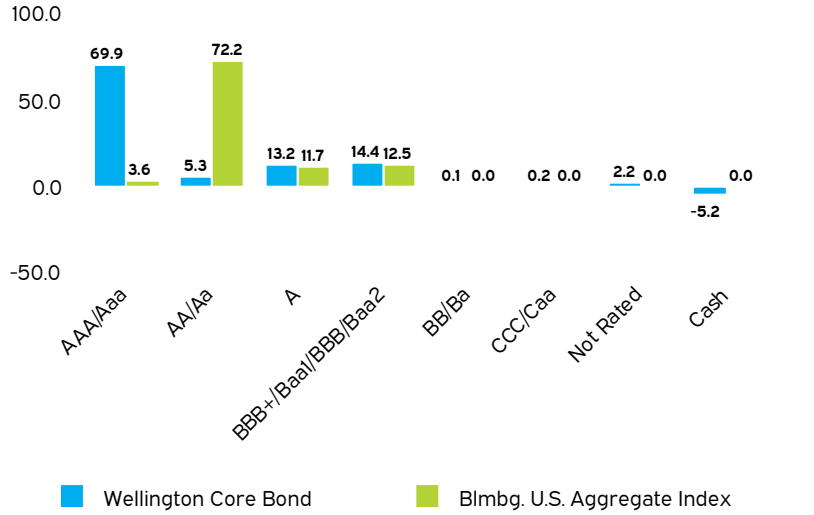


Wellington Core Bond | As of December 31, 2023

Account Information

Account Name	Wellington Core Bond
Inception Date	11/01/2022
Account Structure	Mutual Fund
Asset Class	US Fixed Income
Benchmark	Blmbg. U.S. Aggregate Index

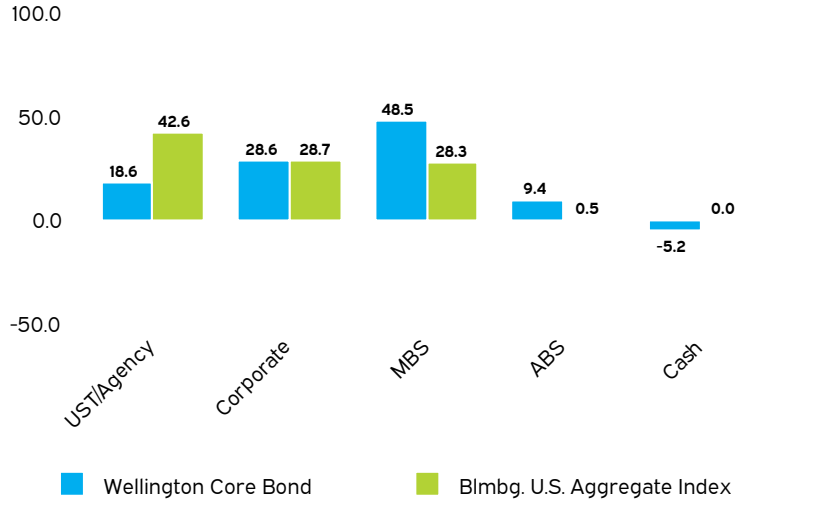
Credit Quality Allocation



Fixed Income Characteristics

	Q4 -23	
	Wellington Core Bond	Blmbg. U.S. Aggregate Inde
Yield To Maturity	4.93	4.53
Average Duration	6.51	6.24
Average Quality	AA	AA
Weight Average Maturity	-	8.46

Sector Distribution

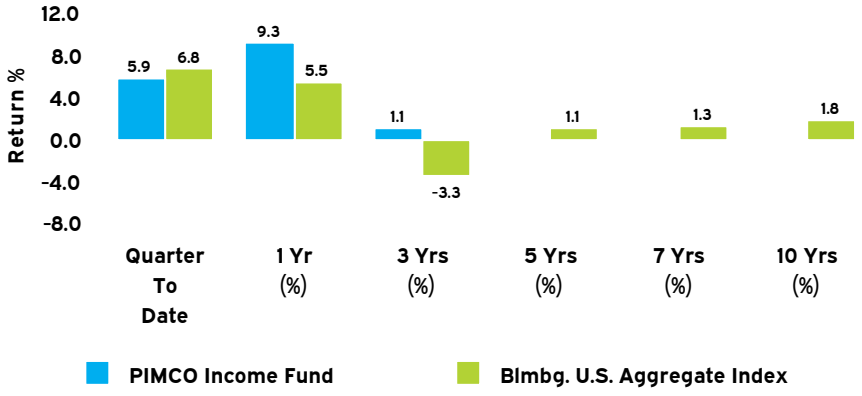


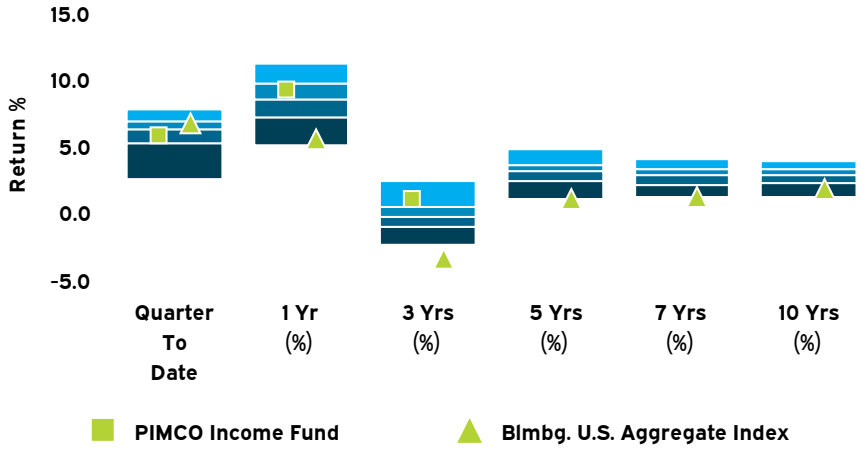
MEKETA

Merced County Employees' Retirement Association

PIMCO Income Fund | As of December 31, 2023

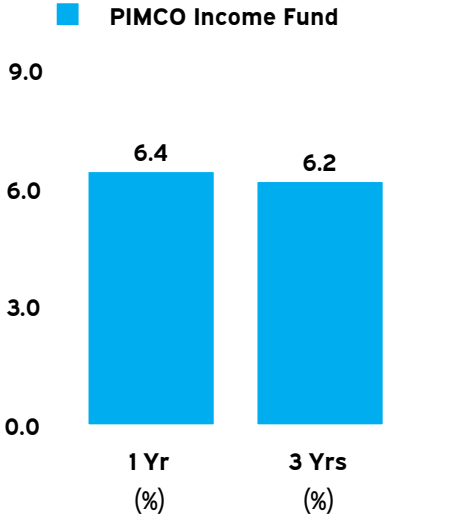
Return Summary



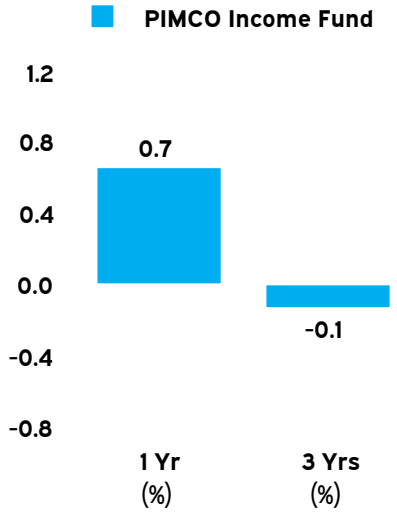


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
PIMCO Income Fund	5.9	9.3	1.1	-	-	-
Blmbg. U.S. Aggregate Index	6.8	5.5	-3.3	1.1	1.3	1.8
Excess Return	-0.9	3.8	4.4	-	-	-

Annualized Standard Deviation



Sharpe Ratio

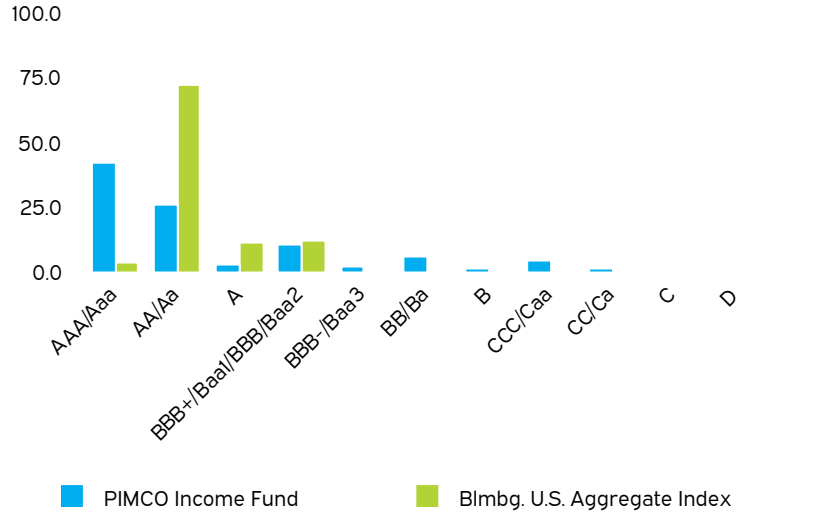


PIMCO Income Fund | As of December 31, 2023

Account Information

Account Name	PIMCO Income Fund
Inception Date	04/30/2019
Account Structure	Mutual Fund
Asset Class	US Fixed Income
Benchmark	Blmbg. U.S. Aggregate Index

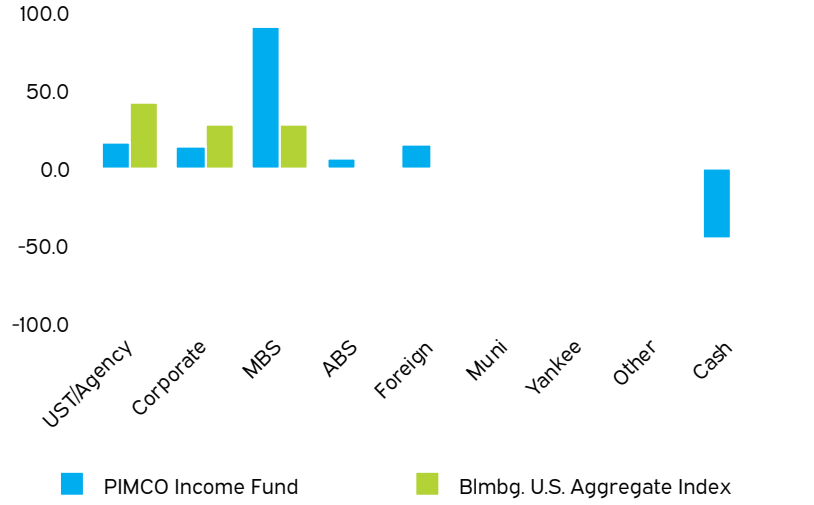
Credit Quality Allocation



Fixed Income Characteristics

	Q4 -23	
	PIMCO Income Fund	Blmbg. U.S. Aggregate Inde
Yield To Maturity	6.54	4.53
Average Duration	3.55	6.24
Average Quality	AAA	AA
Weight Average Maturity	5.31	8.46

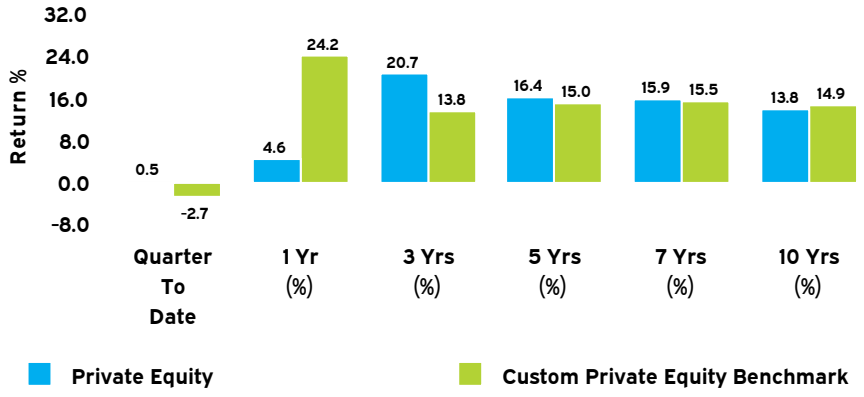
Sector Distribution

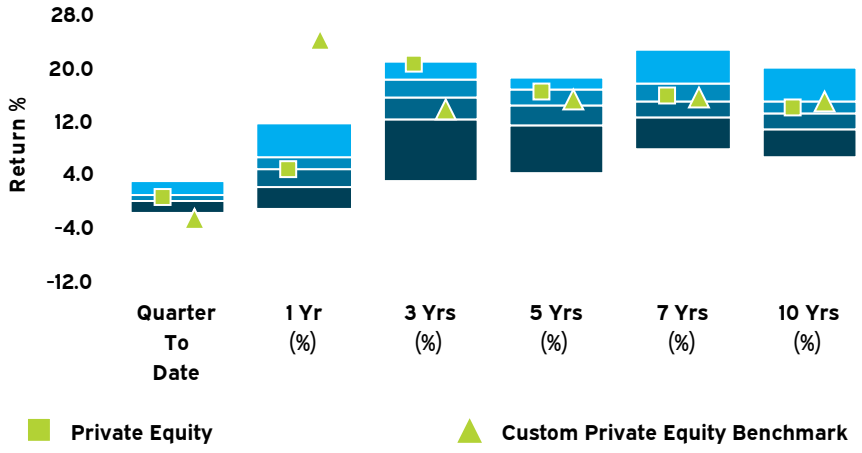


Merced County Employees' Retirement Association

Private Equity | As of December 31, 2023

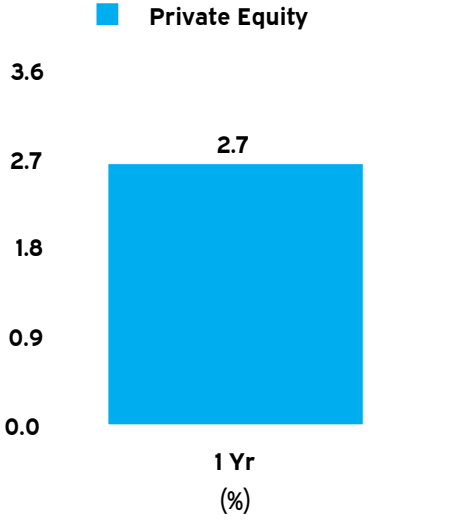
Return Summary



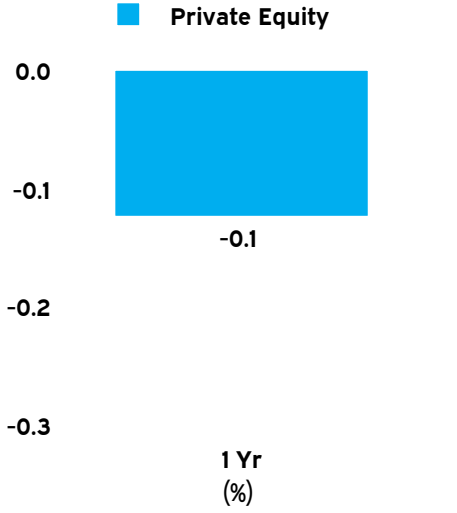


	Quarter To Date	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Private Equity	0.5	4.6	20.7	16.4	15.9	13.8
Custom Private Equity Benchmark	-2.7	24.2	13.8	15.0	15.5	14.9
Excess Return	3.2	-19.6	6.9	1.4	0.4	-1.1

Annualized Standard Deviation



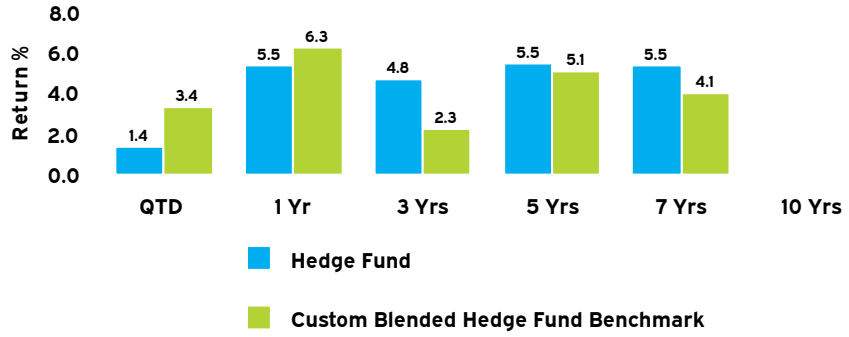
Sharpe Ratio



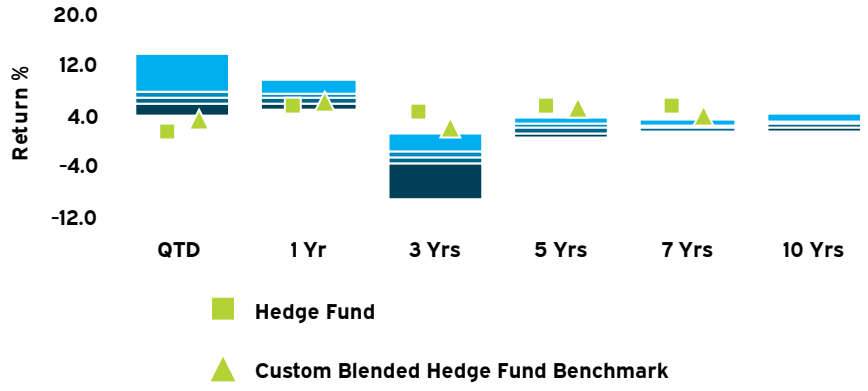
Merced County Employees' Retirement Association

Hedge Fund | As of December 31, 2023

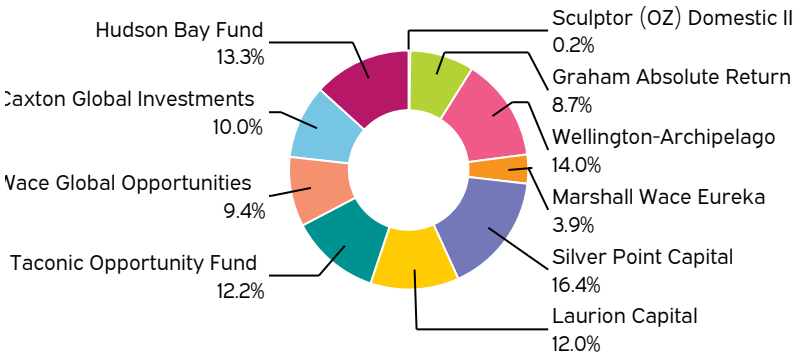
Return Summary



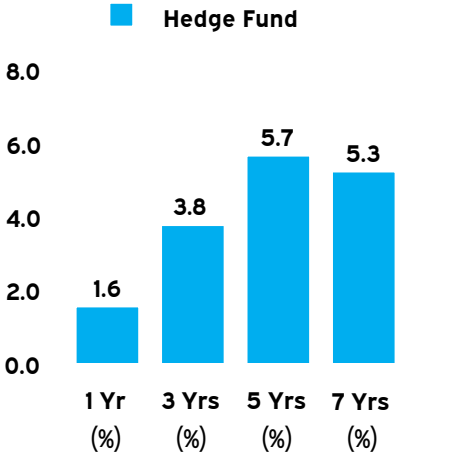
	QTD (%)	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Hedge Fund	1.4	5.5	4.8	5.5	5.5	-
Custom Blended Hedge Fund Benchmark	3.4	6.3	2.3	5.1	4.1	-
Excess Return	-2.0	-0.8	2.5	0.4	1.4	-



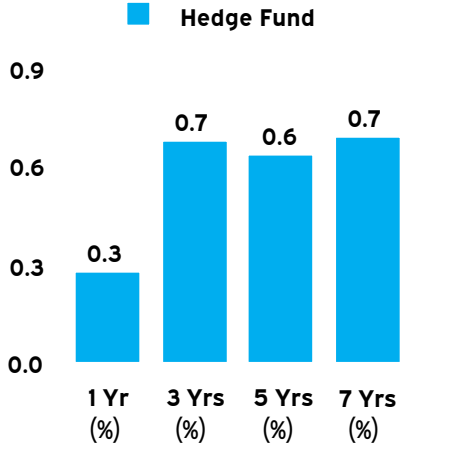
Current Allocation



Annualized Standard Deviation



Sharpe Ratio

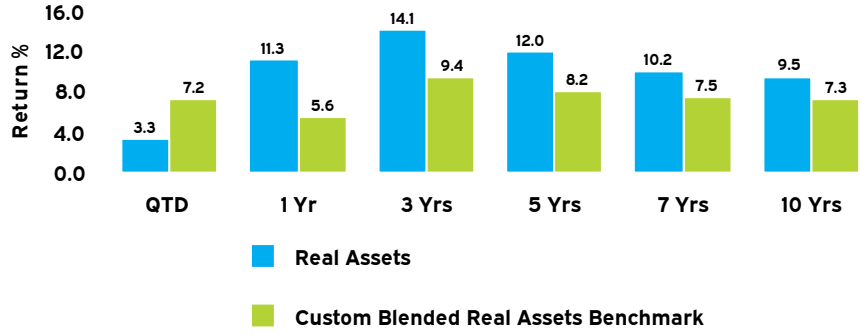


MEKETA

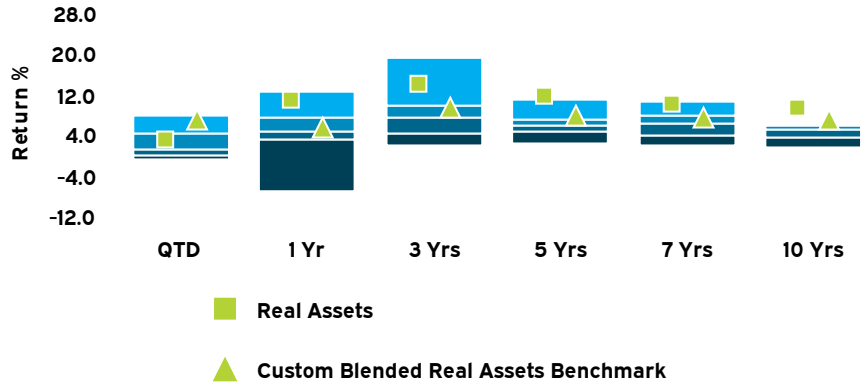
Merced County Employees' Retirement Association

Real Assets | As of December 31, 2023

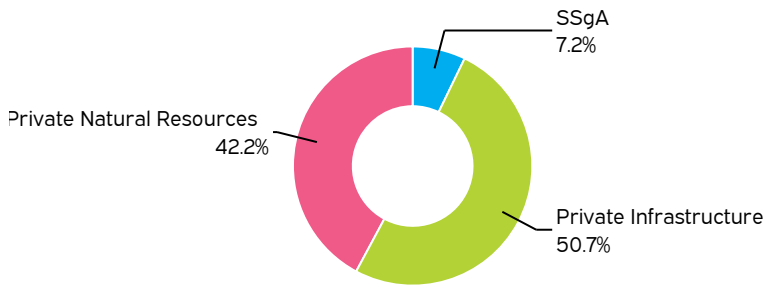
Return Summary



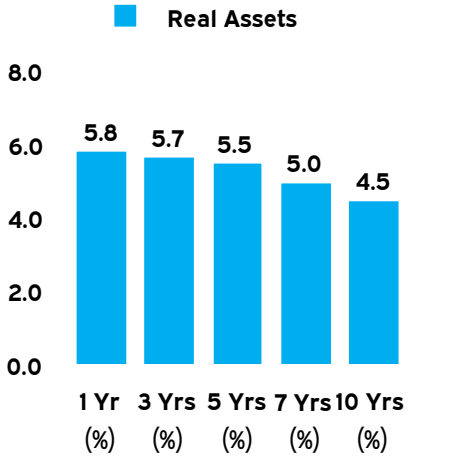
	QTD (%)	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Real Assets	3.3	11.3	14.1	12.0	10.2	9.5
Custom Blended Real Assets Benchmark	7.2	5.6	9.4	8.2	7.5	7.3
Excess Return	-3.9	5.7	4.7	3.8	2.7	2.2



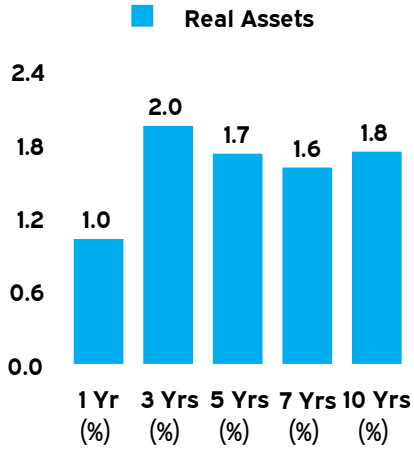
Current Allocation



Annualized Standard Deviation



Sharpe Ratio

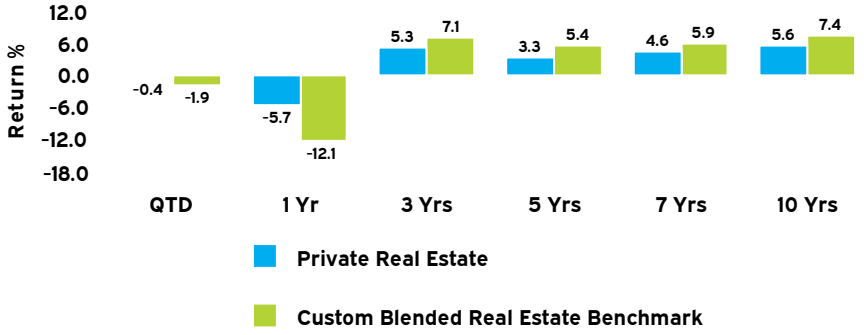


MEKETA

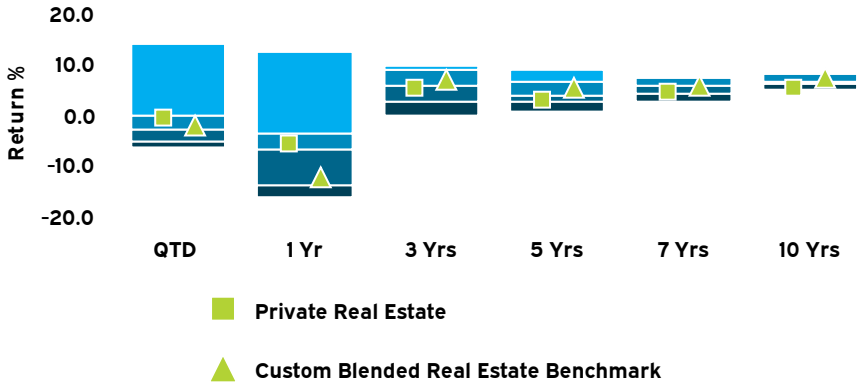
Merced County Employees' Retirement Association

Private Real Estate | As of December 31, 2023

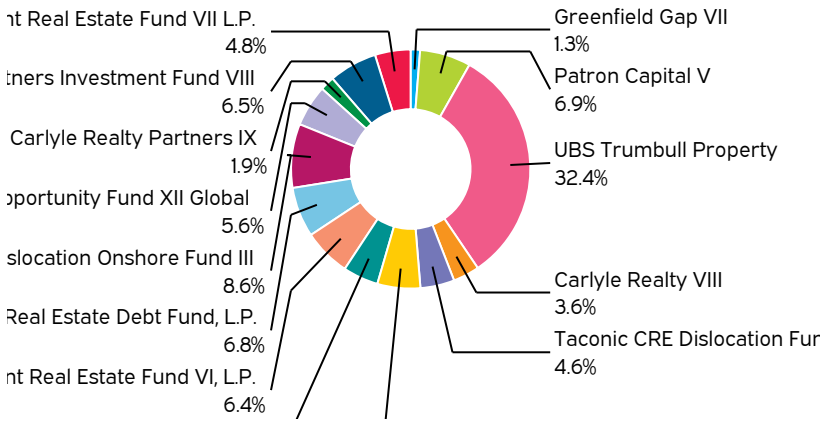
Return Summary



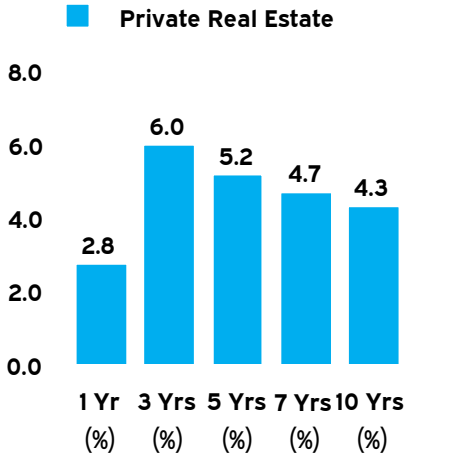
	QTD (%)	1 Yr (%)	3 Yrs (%)	5 Yrs (%)	7 Yrs (%)	10 Yrs (%)
Private Real Estate	-0.4	-5.7	5.3	3.3	4.6	5.6
Custom Blended Real Estate Benchmark	-1.9	-12.1	7.1	5.4	5.9	7.4
Excess Return	1.5	6.4	-1.8	-2.1	-1.3	-1.8



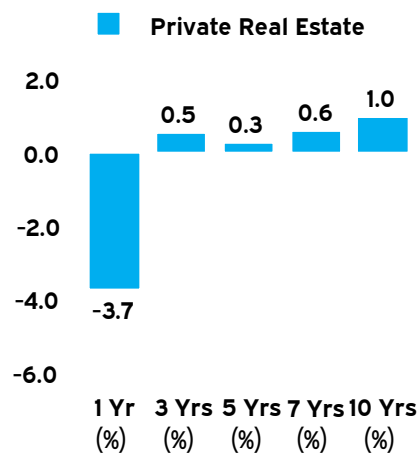
Current Allocation



Annualized Standard Deviation



Sharpe Ratio



Disclaimer, Glossary, and Notes

WE HAVE PREPARED THIS REPORT (THIS "REPORT") FOR THE SOLE BENEFIT OF THE INTENDED RECIPIENT (THE "RECIPIENT").

SIGNIFICANT EVENTS MAY OCCUR (OR HAVE OCCURRED) AFTER THE DATE OF THIS REPORT AND THAT IT IS NOT OUR FUNCTION OR RESPONSIBILITY TO UPDATE THIS REPORT. ANY OPINIONS OR RECOMMENDATIONS PRESENTED HEREIN REPRESENT OUR GOOD FAITH VIEWS AS OF THE DATE OF THIS REPORT AND ARE SUBJECT TO CHANGE AT ANY TIME. ALL INVESTMENTS INVOLVE RISK. THERE CAN BE NO GUARANTEE THAT THE STRATEGIES, TACTICS, AND METHODS DISCUSSED HERE WILL BE SUCCESSFUL.

INFORMATION USED TO PREPARE THIS REPORT WAS OBTAINED FROM INVESTMENT MANAGERS, CUSTODIANS, AND OTHER EXTERNAL SOURCES. WHILE WE HAVE EXERCISED REASONABLE CARE IN PREPARING THIS REPORT, WE CANNOT GUARANTEE THE ACCURACY OF ALL SOURCE INFORMATION CONTAINED HEREIN.

CERTAIN INFORMATION CONTAINED IN THIS REPORT MAY CONSTITUTE "FORWARD - LOOKING STATEMENTS," WHICH CAN BE IDENTIFIED BY THE USE OF TERMINOLOGY SUCH AS "MAY," "WILL," "SHOULD," "EXPECT," "AIM", "ANTICIPATE," "TARGET," "PROJECT," "ESTIMATE," "INTEND," "CONTINUE" OR "BELIEVE," OR THE NEGATIVES THEREOF OR OTHER VARIATIONS THEREON OR COMPARABLE TERMINOLOGY. ANY FORWARD-LOOKING STATEMENTS, FORECASTS, PROJECTIONS, VALUATIONS, OR RESULTS IN THIS PRESENTATION ARE BASED UPON CURRENT ASSUMPTIONS. CHANGES TO ANY ASSUMPTIONS MAY HAVE A MATERIAL IMPACT ON FORWARD - LOOKING STATEMENTS, FORECASTS, PROJECTIONS, VALUATIONS, OR RESULTS. ACTUAL RESULTS MAY THEREFORE BE MATERIALLY DIFFERENT FROM ANY FORECASTS, PROJECTIONS, VALUATIONS, OR RESULTS IN THIS PRESENTATION.

PERFORMANCE DATA CONTAINED HEREIN REPRESENT PAST PERFORMANCE. PAST PERFORMANCE IS NO GUARANTEE OF FUTURE RESULTS.

Credit Risk: Refers to the risk that the issuer of a fixed income security may default (i.e., the issuer will be unable to make timely principal and/or interest payments on the security).

Duration: Measure of the sensitivity of the price of a bond to a change in its yield to maturity. Duration summarizes, in a single number, the characteristics that cause bond prices to change in response to a change in interest rates. For example, the price of a bond with a duration of three years will rise by approximately 3% for each 1% decrease in its yield to maturity. Conversely, the price will decrease 3% for each 1% increase in the bond's yield. Price changes for two different bonds can be compared using duration. A bond with a duration of six years will exhibit twice the percentage price change of a bond with a three-year duration. The actual calculation of a bond's duration is somewhat complicated, but the idea behind the calculation is straightforward. The first step is to measure the time interval until receipt for each cash flow (coupon and principal payments) from a bond. The second step is to compute a weighted average of these time intervals. Each time interval is measured by the present value of that cash flow. This weighted average is the duration of the bond measured in years.

Information Ratio: This statistic is a measure of the consistency of a portfolio's performance relative to a benchmark. It is calculated by subtracting the benchmark return from the portfolio return (excess return), and dividing the resulting excess return by the standard deviation (volatility) of this excess return. A positive information ratio indicates outperformance versus the benchmark, and the higher the information ratio, the more consistent the outperformance.

Jensen's Alpha: A measure of the average return of a portfolio or investment in excess of what is predicted by its beta or "market" risk. Portfolio Return- [Risk Free Rate+Beta*(market return-Risk Free Rate)].

Market Capitalization: For a firm, market capitalization is the total market value of outstanding common stock. For a portfolio, market capitalization is the sum of the capitalization of each company weighted by the ratio of holdings in that company to total portfolio holdings; thus it is a weighted-average capitalization. Meketa Investment Group considers the largest 65% of the broad domestic equity market as large capitalization, the next 25% of the market as medium capitalization, and the smallest 10% of stocks as small capitalization.

Market Weighted: Stocks in many indices are weighted based on the total market capitalization of the issue. Thus, the individual returns of higher market-capitalization issues will more heavily influence an index's return than the returns of the smaller market-capitalization issues in the index.

Maturity: The date on which a loan, bond, mortgage, or other debt/security becomes due and is to be paid off.

Prepayment Risk: The risk that prepayments will increase (homeowners will prepay all or part of their mortgage) when mortgage interest rates decline; hence, investors' monies will be returned to them in a lower interest rate environment. Also, the risk that prepayments will slow down when mortgage interest rates rise; hence, investors will not have as much money as previously anticipated in a higher interest rate environment. A prepayment is any payment in excess of the scheduled mortgage payment.

Price-Book Value (P/B) Ratio: The current market price of a stock divided by its book value per share. Meketa Investment Group calculates P/B as the current price divided by Compustat's quarterly common equity. Common equity includes common stock, capital surplus, retained earnings, and treasury stock adjusted for both common and nonredeemable preferred stock. Similar to high P/E stocks, stocks with high P/B's tend to be riskier investments.

Price-Earnings (P/E) Ratio: A stock's market price divided by its current or estimated future earnings. Lower P/E ratios often characterize stocks in low growth or mature industries, stocks in groups that have fallen out of favor, or stocks of established blue chip companies with long records of stable earnings and regular dividends. Sometimes a company that has good fundamentals may be viewed unfavorably by the market if it is an industry that is temporarily out of favor. Or a business may have experienced financial problems causing investors to be skeptical about is future. Either of these situations would result in lower relative P/E ratios. Some stocks exhibit above-average sales and earnings growth or expectations for above average growth. Consequently, investors are willing to pay more for these companies' earnings, which results in elevated P/E ratios. In other words, investors will pay more for shares of companies whose profits, in their opinion, are expected to increase faster than average. Because future events are in no way assured, high P/E stocks tend to be riskier and more volatile investments. Meketa Investment Group calculates P/E as the current price divided by the I/B/E/S consensus of twelve-month forecast earnings per share.

Quality Rating: The rank assigned a security by such rating services as Fitch, Moody's, and Standard & Poor's. The rating may be determined by such factors as (1) the likelihood of fulfillment of dividend, income, and principal payment of obligations; (2) the nature and provisions of the issue; and (3) the security's relative position in the event of liquidation of the company. Bonds assigned the top four grades (AAA, AA, A, BBB) are considered investment grade because they are eligible bank investments as determined by the controller of the currency.

Sharpe Ratio: A commonly used measure of risk-adjusted return. It is calculated by subtracting the risk free return (usually three-month Treasury bill) from the portfolio return and dividing the resulting excess return by the portfolio's total risk level (standard deviation). The result is a measure of return per unit of total risk taken. The higher the Sharpe ratio, the better the fund's historical risk adjusted performance.

STIF Account: Short-term investment fund at a custodian bank that invests in cash-equivalent instruments. It is generally used to safely invest the excess cash held by portfolio managers.

Standard Deviation: A measure of the total risk of an asset or a portfolio. Standard deviation measures the dispersion of a set of numbers around a central point (e.g., the average return). If the standard deviation is small, the distribution is concentrated within a narrow range of values. For a normal distribution, about two thirds of the observations will fall within one standard deviation of the mean, and 95% of the observations will fall within two standard deviations of the mean.

Style: The description of the type of approach and strategy utilized by an investment manager to manage funds. For example, the style for equities is determined by portfolio characteristics such as price-to-book value, price-to-earnings ratio, and dividend yield. Equity styles include growth, value, and core.

Tracking Error: A divergence between the price behavior of a position or a portfolio and the price behavior of a benchmark, as defined by the difference in standard deviation.

Yield to Maturity: The yield, or return, provided by a bond to its maturity date; determined by a mathematical process, usually requiring the use of a "basis book." For example, a 5% bond pays $5 a year interest on each $100 par value. To figure its current yield, divide $5 by $95—the market price of the bond—and you get 5.26%. Assume that the same bond is due to mature in five years. On the maturity date, the issuer is pledged to pay $100 for the bond that can be bought now for $95. In other words, the bond is selling at a discount of 5% below par value. To figure yield to maturity, a simple and approximate method is to divide 5% by the five years to maturity, which equals 1% pro rata yearly. Add that 1% to the 5.26% current yield, and the yield to maturity is roughly 6.26%.

$$\frac{\text{5\% (discount)}}{\text{5 (yrs. to maturity)}} = \text{1\% pro rata, plus 5.26\% (current yield)} = \text{6.26\% (yield to maturity)}$$

Yield to Worst: The lowest potential yield that can be received on a bond without the issuer actually defaulting. The yield to worst is calculated by making worst-case scenario assumptions on the issue by calculating the returns that would be received if provisions, including prepayment, call, or sinking fund, are used by the issuer.

NCREIF Property Index (NPI): Measures unleveraged investment performance of a very large pool of individual commercial real estate properties acquired in the private market by tax-exempt institutional investors for investment purposes only. The NPI index is capitalization-weighted for a quarterly time series composite total rate of return.

NCREIF Fund Index - Open End Diversified Core Equity (NFI-ODCE): Measures the investment performance of 28 open-end commingled funds pursuing a core investment strategy that reflects funds' leverage and cash positions. The NFI-ODCE index is equal-weighted and is reported gross and net of fees for a quarterly time series composite total rate of return.

Sources: Investment Terminology, International Foundation of Employee Benefit Plans, 1999.
The Handbook of Fixed Income Securities, Fabozzi, Frank J., 1991

Throughout this report, numbers may not sum due to rounding.

Returns for periods greater than one year are annualized throughout this report.

Values shown are in millions of dollars, unless noted otherwise.

County Of Merced

IT Information Security Policies

Forward

Merced County IT Information Security Policies are based on the work of the California County Information Services Directors Association (CCISDA) Information Security Forum (ISF). The CCISDA ISF originally published its 'Information Security Program' in 2003 and released and updated draft in April 2016. The 2016 draft program consisted of templates, based on industry best practices, that counties could adapt and implement locally. The templates were designed to address the modern threat landscape and to be compliant with current Federal and State standards.

The Department of Administrative Services, in coordination with stakeholder departments that were identified as having high-level security requirements, formed the Merced County Information Security Advisory Committee (MCISAC) in 2017 to begin the process of adapting the ISF provided templates to the specific needs of Merced County departments.

The policies must be reviewed and updated to ensure they continue to incorporate industry best practices necessary to defend against ever-evolving threats.

Contributing Members to the Merced County Information Security Advisory Committee

Anthony Prieto, Behavior Health and Recovery Services

Sean Pamer, Human Services Agency

Kirt Craig, Behavior Health and Recovery Services

Yadira Vazquez, Department of Public Health

Kevin Reid, Sheriff Office

John Nishihama, Administrative Services

Ken Kobashigawa, Administrative Services

Rob Kuhlemeier, Administrative Services

Trish Goodman, District Attorney's Office

Linda Jones, District Attorney's Office

Table of Contents

Executive Summary

Introduction

The rapid pace of technological evolution continues to be astounding. We have witnessed the dissolution of the traditional network perimeter and the emergence of the IoT (Internet of Things), cloud computing (and with it 'shadow IT'), virtualization, smart phones, VoIP, and social networking to name a few. Along with these technologies has come the evolution in the sophistication and veracity of malicious attacks.

Information security policies are the cornerstones of an effective information security program. Chasing after vulnerabilities is a far less effective approach than proactively protecting and safeguarding against them. Not providing employees and our organization with the "do's and don't's" of what is expected of them in their operational and strategic activities, leaves them unable to be proactive, raising the risk of potential security incidents.

The policies described in this document will assist the County's IT department in establishing proven industries standards for policy implementation, and allow for the consistent procedures for use of the corresponding IT assets and to harden (secure and readily available) the County's IT infrastructure from errors and omissions, internal and external threats and malicious code.

What are Information Technology Policies and Why Have Them?

Information Technology (IT) security policies are designed to allow IT organizations to establish consistent behavior in their enterprises as well as providing guidelines to information owners (usually County departments) on how their informational assets can and should be managed. IT information security policies help IT organizations build comprehensive procedures which directly build cost efficiencies and manage effectiveness of the IT infrastructure under their control. IT organizations, as the information custodian for the information owners, desire to provide IT goods and services in a meaningful and due diligent manner to all of their stake holders. IT Information security policies will ensure that these capabilities can be met in an ongoing manner. They will help the IT department build and maintain IT infrastructure that provides availability of the information under their control, ensuring that that information maintains integrity and can be trusted, and to ensure that the information owners are in compliance with local, state, and federal regulations and laws as it pertains to their information.

Every organization (private or public) has policies that direct employees and customers on what can and should be expected from the organization. County government is no exception. Policies allow people to understand what is expected of them, and what they are accountable for.

Most policies are based upon law or moral and ethical conducts. The IT information security policies within this document go well beyond those issues by establishing best practices for Merced County's IT department in handling information under their watchful guidance.

Like all policies, the IT information security policies must be implemented and enforceable, concise and easy to understand, and balance protection with productivity. The policies within this document accomplish that. They are drafted using industry proven standards and are developed to allow Merced County the ability to comply with the various laws (Federal, State, and Local) as well as ensure that taxpayer's assets are being used according to the laws and local jurisdictions.

Stability in IT Infrastructure

Imagine what might happen if…

Essential data were stolen, lost, compromised, corrupted, or deleted?

Emergency 911 systems were down for a day or more? What would the cost of life safety be?

Citizens were unable to get County supplied services, such as child support, financial assistance, or health care?

Business disruptions have now developed as the norm for IT organizations. County governments are no exception to this current worldwide trend. Countless thousands of 'attacks' are made against local government each and every day. Without the proper layering of security functionality in place today, IT organizations would not be able to maintain any of their customer's systems. Even before the September 11, 2001 attack on the United States at the World Trade Center and Pentagon, IT systems were under constant attack. A term more reflective of our current

environment, Cyber Security, has been coined to describe the proliferation of the Internet in businesses and personal use.

Cyber Security encompasses both physical and logical security, with emphasis on the logical side. A significant portion of this nation's infrastructure is interconnected through the Internet (thus Cyber). This infrastructure is critical in maintaining our electrical grids, controlling dams, signals, bridges, chemical plants, railroads, shipyards, and the list goes on. In one form or another, this national infrastructure is now intertwined in all governmental businesses processes, so government must also maintain security and robust systems, or we become the weak link in the chain.

Software companies continue to sell their products with major flaws today, which directly put their users at risk. We do not see any immediate remedies for this, as the software industries are not being held directly accountable for selling faulty products. IT organizations then, must do everything in their power to fix these flaws in an expedient manner. This process of discovering that software requires ongoing patches and monitoring that fragile infrastructure has forced IT organizations away from their original missions (providing IT goods and services to their customers). The Merced County IT department has built an infrastructure that is more proactive, trained and organized staff in a manner that allows them to be quick on their feet, and able to grasp the larger picture of the overall businesses they support. No longer can an IT organization have niche functions as these are now related and dependent upon each other for functionality.

IT information security polices help the IT department build and maintain systems and applications that take into consideration dependencies on others, as well as interoperability requirements. IT information security policies that are built on government best practices will guide the IT department toward the establishment of secure systems, that users can and do depend on every day to make the decisions for the organizations as a whole. Having countywide IT Information Security Policies, all built on government best practices, will ensure that the IT department is making their systems reliable to all stakeholders. This can only be viewed as a win/win position, as everyone truly wins at ensuring goods and services are delivered in the most cost effective manner.

IT Information Security Policies, an Executive Perspective

Purposes of IT Policies

The main purpose of IT information security policies is to inform all impacted parties, especially the IT staff, of their obligatory requirements for protecting technology and information assets. The policies should help identify the procedures through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. Therefore, an attempt to use a set of tools in the absence of at least an implied IT information security policy is futile.

Who should be Involved When Forming Policy?

In order for IT information security policies to be appropriate and effective, they need to have the acceptance and support of all levels of employees within the organization. This is true for any policy in an organization. It is especially important that county management and appointed and elected officials fully support the information technology security policy process; otherwise there is little chance that they will have the intended impact. The following is a list of individuals who should be involved in the creation and/or review and approval of information technology security policy documents:

Chief Information Officer, including Information Technology staff (e.g., staff from all elements of computer operational support units)

Department Heads and Elected Officials and administrators of groups within the organization (e.g., business departments as Information Owners)

Merced County Information Security Advisory Committee (MCISAC)

Information Technology Advisory Committee

Executive Management

Other responsible management

Legal Counsel

Human Resources

Employee Unions (for notification purposes only or as appropriate)

The idea is to bring in representation and buy-in from key stakeholders, management who have budget and policy authority, technical staff who know what can and cannot be supported, and legal counsel who know the legal ramifications of various policy choices.

What Makes a Good IT Information Security Policy?

The characteristics of good policies are:

- They must be able to be implemented through both technical and non-technical procedures.
- They must be enforceable with appropriate security and management tools, to include sanctions where actual prevention is not technically feasible.
- They must clearly define the areas of responsibility for users, administrators, management and all IT staff.

Countywide policies include the following subject areas, at a minimum:

- Infrastructure stability, and cost effective resource management
- Systems and Applications Availability
- Standard configurations, backups, and recovery

These policies will allow the IT department the ability to build and maintain an IT infrastructure that is stable and robust, that ultimately will ensure that county government departments can maintain services to their citizenry. These policies allow IT to establish both strategic and tactical plans that meet the overall objectives and goals of the County.

Like all other policies, staff needs to be exposed to these policies in much a manner as they understand them, and will strive to ensure they are followed.

Conclusion

Like any other policy process, executive sponsorship and support are essential for these policies to be successful and accomplish the desired results. IT staff today need to ensure that prevention of incidents is part of their overall behavior. These policies, drafted by the Merced County Information Security Advisory Committee (MCISAC), based on work of the California Counties Information Services Directors Association's (CCISDA) Information Security Form (ISF), are meant to allow Merced County's IT department the ability to ensure consistent behavior and performance in management and strategic direction of the County's Information Technology resources.

Merced County's IT Information Security Policies, contained within this document, support the County's efforts in providing availability, integrity and confidentiality of all county controlled assets, both logical and physical. These policies are based upon industry and governmental 'best practices'. This document support Merced County's goal to foster, build and maintain both effective and efficient methods to safeguard IT assets under County control.

Information Technology Security Policies

Introduction

Today's information technology offers improved communication, and as such, the more complicated our IT environments, the more difficult it is to protect that infrastructure. IT systems continue to become much more robust, yet the trade-off here is that we begin to have disparate systems that by design, make them hard to manage as a collective set of systems. Each system requires staff that essentially has training and experience in that niche. Gone are the days that IT systems were simple to administer, using a standard (typically one vendor) set of software and hardware. With the decentralization of software and hardware, and vendor competition, IT staff has had to become experts in a whole host of various systems and architectures. Include in this complexity, a world of 'hackers' that want to be successful in the penetration of our IT systems and for financial gain or notoriety. To complicate things further, include a vendor base that has yet to agree on an industry standard, as standardization may gradually improve one vendor's product line or that of a competitive vendor. That is to say that they have to create products that can and do interface with their competitors' products.

IT organizations that adopt these best practices lower their overall risks to today's IT implementations and functionalities. It will also force a competitive and often combatant vendor industry to ensure their products mitigate the risk to those using their products thereby minimizing the overall risk to our governmental assets.

People are increasingly dependent on information technology, so it is important to protect technology and encourage its appropriate use. Information technology has diversified over the years, but information-handling requirements have remained relatively consistent. People need to communicate via voice, video, paper, images, and data. Because information must be protected in whatever form it takes, it is important to consider IT security-related issues with paper, surface mail and even presentations at public conferences. IT information security policies must then address the technical methods of handling information.

Merced County and its departments should adopt commonly accepted IT information security best practices since they directly reflect concurrence among information security professionals and industry technological experts. Further, these best practices should be adopted and implemented without change because not to do so could introduce unforeseen risks.

The IT Information Security Policies within this document must apply to all employees, both permanent and temporary, and all contractors, consultants, vendors, interns, volunteers and others who use the resources that are either owned or leased by the county.

Purpose

There are at least four major reasons for implementing these policies:

- Policies set the stage for appropriate behavior and awareness of acceptable IT business practices;
- They help IT staff operate information-handling systems in a secure manner;
- They assist administrators and developers in the implementation and configuration of secure information-handling systems; and,
- They provide managers a means for determining whether new requirements are adhered to, or necessitate a change in, current policy.

The Policies

The policies contained in this document are based on NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations. NIST 800-53 Rev. 4 is a framework and regulatory document, encompassing the processes and controls needed for a government-affiliated entity to comply with Federal Information Processing Standard (FIPS) 200. NIST 800-53 Rev. 4 has been recently updated to reflect the evolving technology and threat space. Areas include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threat; and trustworthiness, assurance, and resilience of information systems. This framework was chosen as a basis for the policies since it is the Federal standard that has also been adopted by the State of California. As such, the County's intent and

hope is that that adoption of these policies will aid in the creation of future MOUs and agreements between the State of California and Merced County.

The 800-53 Rev. 4 controls are divided into the following 17 families:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

NIST 800-53 Rev. 4 contains three levels of controls: Low, Moderate and High. The policies included in this document were derived from the 'Moderate' controls since 'Low" was considered too weak and 'High' too onerous for Merced County. Some controls may have been determined to be not-feasible due to current fiscal, or technical reasons.

Security and Privacy Control Catalog Compliance Mapping

Also contained in the document is a matrix titled *Security and Privacy Control Catalog Compliance Mapping*. The matrix is a direct mapping between NIST 800-53 Rev. 4, the SANS 20 Critical Controls, ISO 27001, SAM, IRS, and HIPAA controls.

Policy #:	Title:	Effective Date:
1.0	Access Control Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) implements access controls in compliance with County IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Access Control (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164;
NIST Federal Information Processing Standards (FIPS) 199;
State of California **State Administrative Manual (SAM) 5300 et seq.,** Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. ACCOUNT MANAGEMENT
   County IT and or Designated Departmental Staff shall:

   a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

   b. Assign account managers for information system accounts.

   c. Establish conditions for group and role membership.

   d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

   e. Require approvals by departmental system owners for requests to create information system accounts.

   f. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.

   g. Monitor the use of information system accounts.

   h. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.

   i. Authorize access to the information system based on a valid access authorization or intended system usage.

   j. Review accounts for compliance with account management requirements. Monthly reports will be automatically generated and distributed for review and action.

   k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

   l. Employ automated mechanisms to support the management of information system accounts.
   m. Ensure that the information system automatically disables temporary and emergency accounts after usage.

n. Ensure that the information system automatically disables inactive accounts after 90 days.

o. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

2. ACCESS ENFORCEMENT
County IT shall:

a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

3. INFORMATION FLOW ENFORCEMENT
County IT shall:

a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

4. SEPARATION OF DUTIES
County IT shall:

a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

b. Document the separation of duties of individuals.

c. Define information system access authorizations to support separation of duties.

5. LEAST PRIVILEGE
County IT shall:

a. Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

b. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

c. Require that users of information system accounts, or roles, with access to information system accounts, use non-privileged accounts or roles, when accessing non-security functions.

d. Restrict privileged accounts on the information system to administrative groups managed by Active Directory.

e. Ensure that the information system audits the execution of privileged functions.

f. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

6. UNSUCCESSFUL LOGON ATTEMPTS
County IT shall ensure that the information system:

a. Enforces a limit of consecutive invalid logon attempts by a user during a 1 Hour period

b. Locks the account/node automatically for 10 Minutes or until released by an administrator when the maximum number of unsuccessful attempts is exceeded. Each Department

may have variations to the time period of locked accounts dependent upon departmental requirement.

7. SYSTEM USE NOTIFICATION
   County IT shall ensure that the information system:

   a. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:

      i. Users are accessing a County information system.

      ii. Information system usage may be monitored, recorded, and subject to audit.

      iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

      iv. Use of the information system indicates consent to monitoring and recording.

      v. There are not rights to privacy.

   b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

   c. For publicly accessible systems, County IT shall ensure that the information system:

      i. Displays system use information specified by the County Department, before granting further access.

      ii. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

      iii. Includes a description of the authorized uses of the system.

8. SESSION LOCK
   County IT shall ensure that the information system:

   a. Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user. Department session lock time may vary as departments may have policies dictating a shorter lock time.

   b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

   c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

9. SESSION TERMINATION
   County IT shall:

   a. Ensure that the information system or application automatically terminates a user session after 1 hour. Department session termination time may vary as departments may have policies dictating a shorter session termination time.

10. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
    County IT shall:

    a. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.

    b. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

The County IT and Departments shall permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.

11. REMOTE ACCESS
    County IT shall:

    a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

    b. Authorize remote access to the information system prior to allowing such connections.

    c. Ensure that the information system monitors and controls remote access methods.

    d. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

    e. Ensure that the information system routes all remote accesses through the two county managed network access control points to reduce the risk for external attacks (Cisco VPN & Netmotion Mobility).

    f. Authorize the execution of privileged commands and access to security-relevant information via remote access only for assigned County Network Administrators or their designee.

    g. Document the rationale for such access in the security plan for the information system.

12. WIRELESS ACCESS
    County IT shall:

    a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

    b. Authorize wireless access to the information system prior to allowing such connections.

    c. Ensure that the information system protects wireless access to the system using authentication and encryption.

13. ACCESS CONTROL FOR MOBILE DEVICES
    County IT shall:

    a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

    b. Authorize the connection of mobile devices to organizational information systems.

    c. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.

Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical

locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family.

14. USE OF EXTERNAL INFORMATION SYSTEMS
    County IT shall:

    a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

        i. Access the information system from external information systems.

        ii. Process, store, or transmit organization-controlled information using external information systems.

    b. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

        i. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

        ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

15. INFORMATION SHARING
    County IT shall:

    a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for County defined information sharing circumstances where user discretion is required.

    b. Employ County defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

    c. Departments shall determine the extent of information shared employing the principles of least privilege.

16. PUBLICLY ACCESSIBLE CONTENT
    County IT or Designated Departmental Staff shall:

    a. Designate individuals authorized to post information onto a publicly accessible information system – including, but not limited to, Social Media in accordance with the adopted County Social Media Policy.

    b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information. County Departments will provide additional training to ensure staff understand how this applies to each department.

    c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

d. Review the content on the publicly accessible information system for nonpublic information as requests for publications are submitted, and removes such information, if discovered.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
2.0	County Security Awareness and Training Policy	7/1/2017

PURPOSE

To ensure that the appropriate level of information security awareness training is provided to all County Information Technology (IT) users.

REFERENCES

National Institute of Standards and Technology (NIST) Special Publications: NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100;
Electronic Code of Federal Regulations (CFR): 5 CFR 930.301;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. SECURITY AWARENESS TRAINING
   The County shall:

   a. Schedule security awareness training as part of initial training for new users.

   b. Schedule security awareness training when required by information system changes and then annually thereafter.

   c. County IT and County Departments shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

      i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

      ii. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

2. SECURITY AWARENESS | INSIDER THREAT
   County IT and County Departments shall:

   a. Include security awareness training on recognizing and reporting potential indicators of insider threat.

3. ROLE-BASED SECURITY TRAINING
   County IT and County Departments shall:

   a. Provide role-based security training to personnel with assigned security roles and responsibilities:

      i. Before authorizing access to the information system or performing assigned duties.

      ii. When required by information system changes and every two years thereafter.

b. Designate County personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

4. PHYSICAL SECURITY CONTROLS
   County IT and County Departments shall:

   a. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).

   b. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

5. PRACTICAL EXERCISES
   County IT and County Departments shall:

   a. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

6. SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR
   County IT and County Departments shall:

   a. Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

7. SECURITY TRAINING RECORDS
   The County and County Departments shall:

   a. Designate County personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

   b. Retain individual training records for as long as regulations require.

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
3.0	Auditing and Accountability Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Auditing and Accountability (AU), NIST SP 800-12, NIST SP 800-92, NIST SP 800-100;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. AUDIT EVENTS
   The information systems owners, in cooperation with audits and IT, shall:

   a. Determine that the information system is capable of auditing the following events:

      i. Audit account logon events – Success and Failure
      ii. Audit account management – Success and Failure
      iii. Audit directory services access – Success and Failure
      iv. Audit logon events - Success and Failure
      v. Audit object access - Success and Failure (this item only add to logs when
      vi. auditing is enabled on specific files or other objects)
      vii. Audit policy change - Success and Failure
      viii. Audit privilege use - Success and Failure
      ix. Audit process tracking - Success and Failure
      x. Audit system events - Success and Failure

   b. Coordinate the security audit function with other organizational entities requiring audit.

   c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

   d. Determine that the following events are to be audited within the information system:

      i. Audit account logon events – Success and Failure
      ii. Audit account management – Success and Failure
      iii. Audit logon events - Success and Failure
      iv. Audit object access - Success and Failure
      v. Audit policy change - Success and Failure
      vi. Audit system events - Success and Failure

2. REVIEWS AND UPDATES

   a. The organization shall review and update the audited events monthly.

3. CONTENT OF AUDIT RECORDS

   a. The information system shall generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

4. ADDITIONAL AUDIT INFORMATION

    a. The information system shall generate audit records containing the additional information requested by Departments which are unique to their requirements.

5. AUDIT STORAGE CAPACITY

    a. The information owner shall ensure audit record storage capacity is allocated in accordance with State and Federal Regulations. County Departments will coordinate the storage and retention of records.

6. TRANSFER TO ALTERNATE STORAGE

    a. The information system shall off-load audit records daily, weekly and monthly onto a different system or media than the system being audited.

7. RESPONSE TO AUDIT PROCESSING FAILURES
   The information system shall:

    a. Where defined, alert County IT in the event of an audit failure.

    b. Take the following additional actions: County IT shall ensure that the information system will restore the audit functionality and preserve the last audit records.

8. AUDIT STORAGE CAPACITY

    a. The information system shall provide a warning to County IT Enterprise staff within 24 hours of when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity.

9. REAL-TIME ALERTS

    a. The information system shall provide an alert within 5 minutes to County IT Enterprise staff when designated audit failure events occur.

10. CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

    a. The information system shall enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity and throttle network traffic above those thresholds.

11. SHUTDOWN ON FAILURE

    a. The information system shall invoke a degraded operational mode with limited mission/business functionality available in the event of a County IT or Departmental defined audit failure, unless an alternate audit capability exists.

12. AUDIT REVIEW, ANALYSIS, AND REPORTING
    The information system owner shall:

    a. Review and analyze information system audit records monthly for indications of County defined inappropriate or unusual activity.

    b. Report findings to County IT Information Security Officer.

13. PROCESS INTEGRATION

    a. The information system owners shall ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

14. AUDIT REPOSITORIES

    a. The information system owner shall ensure analysis and correlation of audit records across different repositories to gain county-wide situational awareness.

15. AUDIT REDUCTION AND REPORT GENERATION

    a. The information system shall provide an audit reduction and report generation capability that:

        i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.

        ii. Does not alter the original content or time ordering of audit records.

16. AUTOMATIC PROCESSING

    a. The information system shall provide the capability to process audit records for events of interest based on County IT and Departmental defined audit fields within audit records.

17. TIME STAMPS
    The information system shall:

    a. Use internal system clocks to generate time stamps for audit records.

    b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets County defined granularity of time measurement.

18. SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE
    The information system shall:

    a. Compare the internal information system clocks hourly with NTP.ORG.

    b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 3 minutes.

19. PROTECTION OF AUDIT INFORMATION

    a. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.

20. ACCESS BY SUBSET OF PRIVILEGED USERS

    a. The organization shall authorize access to management of audit functionality to only Network System and Support Analysts with Administrator Privileges.

21. AUDIT RECORD RETENTION

    a. The information system owners shall retain audit records for 1 year or a departmentally defined time period consistent with their records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

22. LONG-TERM RETRIEVAL CAPABILITY

    a. The information system owners shall employ system backups to ensure that long-term audit records generated by the information system can be retrieved.

23. AUDIT GENERATION
    The information system shall:

    a. Provide audit record generation capability for the auditable events as defined at server and application levels.

    b. Allow County IT and Departments to select which auditable events are to be audited by specific components of the information system.

    c. Generate audit records for the events with the content as defined.

24. STANDARDIZED FORMATS

    a. The information system shall produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

25. CHANGES BY AUTHORIZED INDIVIDUALS

    a. The information system shall provide the capability for County IT to change the auditing to be performed on County defined information system components based on selectable event criteria within 24 hours of the request.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
4.0	County Security Assessment and Authorization Policy	07/01/2017

PURPOSE

County Information Technology (IT) and the County's various business units (information owners) will ensure security controls in information systems, and the environments in which those systems operate, as part of initial and ongoing security authorizations, annual assessments, continuous monitoring and system development life cycle activities.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Security Assessment and Authorization (CA), NIST SP 800-12, NIST SP 800-37, NIST SP 800-39, NIST SP 800-47, NIST SP 800-100, NIST SP 800-115, NIST SP 800-137;
NIST Federal Information Processing Standards (FIPS) 199;
State of California: State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets. Every County department that maintains or collects informational assets must be compliant with this policy.

1. SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
   The County shall:

   a. Develop, document, and disseminate to designated departmental representatives:

      i. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

      ii. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.

   b. Review and update the current security assessment and authorization policy and procedures annually.

2. SECURITY ASSESSMENTS
   The County shall:

   a. Develop a security assessment plan that describes the scope of the assessment including:

      i. Security controls and control enhancements under assessment.

      ii. Assessment procedures to be used to determine security control effectiveness.

      iii. Assessment environment, assessment team, and assessment roles and responsibilities.

   b. Assess the security controls in the information system and its environment of operation *quarterly* to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

   c. Produce a security assessment report that documents the results of the assessment.

d. Provide the results of the security control assessment *to designated departmental representatives.*

3. SYSTEM INTERCONNECTIONS
   County IT shall:

   a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements.

   b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

   c. Review and update Interconnection Security Agreements *annually*.

   d. Employ *explicit* policies for allowing *County defined information systems* to connect to external information systems.

4. PLAN OF ACTION AND MILESTONES
   The County shall:

   a. Develop a plan of action and milestones for the information system to document the County's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

   b. Update existing plan of action and milestones *quarterly* based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

5. SECURITY AUTHORIZATION
   The County shall:

   a. Assign a senior-level executive or manager as the authorizing official for the information system.

   b. Ensure that the authorizing official authorizes the information system for processing before commencing operations.

   c. Update the security authorization *annually*.

6. CONTINUOUS MONITORING
   County IT shall:

   a. Develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

      i. Establishment of metrics to be monitored.

      ii. Establishment of *County defined frequencies (Monthly)* for monitoring and *County defined frequencies (Annual)* for assessments supporting such monitoring.

      iii. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

      iv. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.

      v. Correlation and analysis of security-related information generated by assessments and monitoring.

      vi. Response actions to address results of the analysis of security-related information.

vii. Reporting the security status of organization and the information system to *County IT and Departmental representatives.*

7. INTERNAL SYSTEM CONNECTIONS
   County IT shall:

   a. Authorize internal connections of *County defined information system components* to the information system.

   b. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
5.0	Configuration Management Policy	7/1/2017

PURPOSE

To ensure that County Information Technology (IT) resources are inventoried and configured in compliance with County IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Configuration Management (CM);
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. BASELINE CONFIGURATION
   County IT shall:

   a. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.

   b. Review and update the baseline configuration of the information system *monthly.*

   c. Review and update the baseline configuration of the information system when required as a result of *changes made within the information system* and as an integral part of information system component installations and upgrades.

   d. Retain one previous version of baseline configurations of information systems to support rollback.

2. CONFIGURATION CHANGE CONTROL
   County IT shall:

   a. Determine the types of changes to the information system that are configuration-controlled.

   b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.

   c. Document configuration change decisions associated with the information system.

   d. Implement approved configuration-controlled changes to the information system.

   e. Retain records of configuration-controlled changes to the information system for as *long as required by regulations governing information systems.*

   f. Audit and review activities associated with configuration-controlled changes to the information system.

   g. Coordinate and provide oversight for configuration change control activities through *the County Information Services Change Committee that convenes at least on a quarterly basis.*

   h. Test, validate, and document changes to the information system before implementing the changes on the operational system.

3. SECURITY IMPACT ANALYSIS
   County IT shall:

   a. Analyze changes to the information system to determine potential security impacts prior to change implementation.

4. ACCESS RESTRICTIONS FOR CHANGE
   County IT shall:

   a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

5. CONFIGURATION SETTINGS
   County IT shall:

   a. Establish and document configuration settings for information technology products employed within the information system using *various tools and information system management tools* that reflect the most restrictive mode consistent with operational requirements.

   b. Implement the configuration settings.

   c. Identify, document, and approve any deviations from established configuration Settings *County defined information system components* based on *County defined operational requirements*.

   d. Monitor and control changes to the configuration settings in accordance with County policies and procedures.

6. LEAST FUNCTIONALITY
   County IT shall:

   a. Configure the information system to provide only essential capabilities.

   b. Review the information system *quarterly* to identify unnecessary and/or non secure functions, ports, protocols, and services.

   c. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

   d. Prevent program execution in accordance with County policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.

   e. Identify software programs not authorized to execute on information systems.

   f. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

   g. Review and update the list of unauthorized software programs annually.

7. INFORMATION SYSTEM COMPONENT INVENTORY
   County IT shall:

   a. Develop and document an inventory of information system components that:

      i. Reflects the current information system accurately.

      ii. Includes all components within the authorization boundary of the information system.

iii. Is at the level of granularity deemed necessary for tracking and reporting.

iv. Includes information deemed necessary to achieve effective information system component accountability.

b. Review and update the information system component inventory ***monthly.***

c. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.

d. Employ automated mechanisms ***weekly*** to detect the presence of unauthorized hardware, software, and firmware components within the information system.

e. Take the following actions when unauthorized components are detected:

i. Disable network access by such components, or

ii. Isolate the components and notifies the Chief Information Officer and system owner.

f. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

8. CONFIGURATION MANAGEMENT PLAN
County IT shall develop, document, and implement a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures.

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.

c. Defines the configuration items for the information system and places the configuration items under configuration management.

d. Protects the configuration management plan from unauthorized disclosure and modification.

9. SOFTWARE USAGE RESTRICTIONS
County IT shall:

a. Use software and associated documentation in accordance with contract agreements and copyright laws.

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

10. USER-INSTALLED SOFTWARE
County IT shall:

a. Establish policies governing the installation of software by users.

b. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.

c. Monitor policy compliance at as instances are reported by management tools.

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	7/1/2017
Date Reviewed:	7/1/2021

Policy #:	Title:	Effective Date:
6.0	County Contingency Planning Policy	07/01/2017

PURPOSE

To ensure that normal County Information Technology (IT) resources and information systems are available during times of disruption of services.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP):
NIST SP 800-53a – Contingency Planning (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST SP 800-84;
NIST Federal Information Processing Standards (FIPS) 199;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. CONTINGENCY PLAN
   County IT shall:

   a. Develop a contingency plan for the information system, in direct guidance and association with the information system owner, that:

      i. Identifies essential missions and business functions and associated contingency requirements.

      ii. Provides recovery objectives, restoration priorities, and metrics.

      iii. Addresses contingency roles, responsibilities, assigned individuals with contact information.

      iv. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.

      v. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

      vi. Is reviewed and approved by the *Continuity of Operations Plan (COOP) team members*, and information system's owner management on at least an annual basis.

   b. Distribute copies of contingency plans to key contingency personnel, identified by name and/or by business role.

   c. Coordinate contingency planning activities with incident handling activities.

   d. Update the contingency plan to address changes to the business owner's mission, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

   e. Communicate contingency plan changes to key contingency personnel identified by name and/or by business role.

   f. Protect the contingency plan from unauthorized disclosure and modification.

2. CONTINGENCY TRAINING
   County IT shall:

   a. Provide contingency training to information system users (all departments, offices, including the commissions, districts, and Board of Supervisors) consistent with assigned roles and responsibilities

   b. Ensure designated personnel receive contingency training at least biannually of assuming a contingency role or responsibility, and when required by information system changes.

3. CONTINGENCY PLAN TESTING
   County IT, along with County information systems owners, shall:

   a. Test the contingency plan for the information system, as determined by the mission critical nature of the business system(s) no less than annually.

   b. Use strategic and tactical planning during testing to simulate a production information system to determine the effectiveness of the plan and the organizational readiness to execute the plan.

   c. Review the contingency plan test results.

   d. Initiate corrective actions, as needed.

   e. Coordinate contingency plan testing with organizational elements responsible for related plans; plans related to contingency plans for information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans.

4. ALTERNATE STORAGE SITE
   County IT, in direct guidance and association with the County information system owner, shall:

   a. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.

   b. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

   c. Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

   d. Identify and document potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

5. ALTERNATE PROCESSING SITE
   County IT, in direct guidance and association with the County information system owner, shall:

   a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of the information system operations for essential missions/business functions within the time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.

   b. Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the agreed upon time period for transfer/resumption.

c. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.

d. Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

e. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

f. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with County business objectives and availability requirements.

6. TELECOMMUNICATIONS SERVICES
County IT shall:

a. Establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within agreed upon recovery timeframes when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

b. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with agreed upon recovery objectives and availability requirements.

c. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

7. INFORMATION SYSTEM BACKUP
County IT, in direct guidance and association with the County information system owner, shall:

a. Conduct backups of user-level information contained in the information system defined by frequency consistent with recovery time and recovery point objectives.

b. Conduct backups of system-level information contained in the information system defined by frequency consistent with recovery time and recovery point objectives.

c. Conduct backups of information system documentation including security-related documentation defined by frequency consistent with recovery time and recovery point objectives.

d. Protect the confidentiality, integrity, and availability of backup information at storage locations.

e. Test backup information to verify media reliability and information integrity.

8. INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
County IT, in direct guidance and association with the County information system owner, shall:

a. Provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

b. Provide that the information system implements transaction recovery for systems that are transaction-based.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County Information Technology (IT) resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENTS

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	7/1/2017
Date Reviewed:	7/1/2021

Policy #:	Title:	Effective Date:
7.0	Identification and Authentication Policy	7/1/2017

PURPOSE

To ensure that only properly identified and authenticated users and devices are granted access to County Information Technology (IT) resources in compliance with County IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116;
Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors;
Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. IDENTIFICATION AND AUTHENTICATION (County Users)
   Where applicable, County IT shall:

   a. Ensure that information systems uniquely identify and authenticate County users or processes acting on behalf of County users.

   b. Ensure that information systems implement multifactor authentication for network access to privileged accounts.

   c. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.

   d. Ensure that information systems implement multifactor authentication for local access to privileged accounts.

   e. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.

   f. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.

   g. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials.

2. DEVICE IDENTIFICATION AND AUTHENTICATION
   County IT shall:

   a. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

3. IDENTIFIER MANAGEMENT
   County IT, through department information systems owners, shall:

   a. Ensure that the County manages information system identifiers by receiving authorization from *Departmental assigned staff* to assign an individual, group, role, or device identifier.

   b. Select an identifier that identifies an individual, group, role, or device.

   c. Assign the identifier to the intended individual, group, role, or device.

   d. Prevent reuse of identifiers for 90 days.

   e. Disable the identifier after 90 days of inactivity.

4. AUTHENTICATOR MANAGEMENT
   County IT shall:

   a. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

   b. Establish initial authenticator content for authenticators defined by the organization.

   c. Ensure that authenticators have sufficient strength of mechanism for their intended use.

   d. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

   e. Change default content of authenticators prior to information system installation.

   f. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.

   g. Change/refresh authenticators every 90 days.

   h. Protect authenticator content from unauthorized disclosure and modification.

   i. Require individuals and devices to implement specific security safeguards to protect authenticators.

   j. Change authenticators for group/role accounts when membership to those accounts changes.

   k. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.

   l. Ensure passwords must contain characters from three of the following five categories:

      i. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);

      ii. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);

      iii. Base 10 digits (0 through 9);

      iv. Non-alphanumeric characters ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/; and

      v. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

m. Require passwords to have a minimum length of 8 characters.

n. Enforce at least one changed character when new passwords are created.

o. Store and transmit only cryptographically-protected passwords.

p. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.

q. Prohibit password reuse for 12 generations.

r. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

s. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

t. Enforce authorized access to the corresponding private key.

u. Map the authenticated identity to the account of the individual or group.

v. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

w. Departments shall require that the registration process to receive County defined types of and/or specific authenticators be conducted in person; by Personnel Staff before County defined registration authority with authorization by County defined personnel or roles.

x. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy *FIPS 140-2*.

5. AUTHENTICATOR FEEDBACK
   County IT shall:

   a. Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

6. CRYPTOGRAPHIC MODULE AUTHENTICATION
   County IT shall:

   a. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

7. IDENTIFICATION AND AUTHENTICATION (NON-COUNTY USERS)
   County IT shall:

   a. Ensure that information systems uniquely identify and authenticate non-County users or processes acting on behalf of non-County users.

   b. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies *where applicable*.

   c. Ensure that information systems accept Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials *where applicable*.

   d. Ensure that the organization employs FICAM-approved information system components in *County defined information systems* to accept third-party credentials *where applicable.*

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
8.0	Incident Response Policy	7/1/2017

PURPOSE

To ensure that County Information Technology (IT) properly identifies, contains, investigates, remedies, reports, and responds to computer security incidents.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Incident Response (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. INCIDENT RESPONSE TRAINING
   The County shall:

   a. Provide incident response training to information system users consistent with assigned roles and responsibilities:

      i. Within 30 days of assuming an incident response role or responsibility.

      ii. When required by information system changes, and ***annually*** thereafter.

   b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

   c. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

2. INCIDENT RESPONSE TESTING
   The County shall:

   a. Test the incident response capability for the information system ***annually*** using ***County defined tests*** to determine the incident response effectiveness and documents the results.

   b. Coordinate incident response testing with County entity elements responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

3. INCIDENT HANDLING
   The County shall:

   a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

   b. Coordinate incident handling activities with contingency planning activities.

   c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

4. INCIDENT MONITORING
   The County shall:

   a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

5. INCIDENT REPORTING
   The County shall:

   a. Require personnel to report suspected security incidents to the County incident response capability within *8 hours period.*

   b. Report security incident information to County IT.

6. INCIDENT RESPONSE ASSISTANCE
   The County shall:

   a. Provide an incident response support resource, integral to the County incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

7. INCIDENT RESPONSE PLAN
   The County shall:

   a. Develop an incident response plan that:

      i. Provides the County with a roadmap for implementing its incident response capability.

      ii. Describes the structure and County of the incident response capability.

      iii. Provides a high-level approach for how the incident response capability fits into the overall County.

      iv. Meets the unique requirements of the County, which relate to mission, size, structure, and functions.

      v. Defines reportable incidents.

      vi. Provides metrics for measuring the incident response capability within the County.

      vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

      viii. Is reviewed and approved by *County IT – IS Manager or designee*.

   b. Distribute copies of the incident response plan to *County defined incident response personnel (IS Manager, CIO, Department designees).*

   c. Review the incident response plan *annually*.

   d. Update the incident response plan to address system/County changes or problems encountered during plan implementation, execution, or testing.

   e. Communicate incident response plan changes to *County defined incident response personnel (IS Manager, CIO, Department designees).*

   f. Protect the incident response plan from unauthorized disclosure and modification.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	7/1/2017
Date Reviewed:	7/1/2021

Policy #:	Title:	Effective Date:
9.00	Maintenance Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) resources are maintained in compliance with County IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – System Maintenance (MA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-88, NIST SP 800-100;
Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 201;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. CONTROLLED MAINTENANCE
   County IT shall:

   a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or County requirements conducted by local IT and/or outsourced IT entities.

   b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

   c. Require that system owners explicitly approve the removal of the information system or system components from County facilities for off-site maintenance or repairs.

   d. Sanitize equipment to remove all information from associated media prior to removal from county facilities for off-site maintenance or repairs.

   e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

   f. Include County IT and system owner’s defined maintenance-related information in County maintenance records.

   g. For those components not directly associated with information processing such as scanners, copiers, and printers, maintenance records must include date and time of maintenance, entity performing the maintenance, maintenance performed, components replaced or removed including identification/serial numbers as applicable.

2. MAINTENANCE TOOLS
   County IT shall:

   a. Ensure that system owners and County IT approve, control, and monitor information system maintenance tools.

   b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

   c. Check media containing diagnostic and test programs for malicious code before the media are used in the information system.

3. NONLOCAL MAINTENANCE
   County IT shall:

   a. Approve and monitor non-local maintenance and diagnostic activities.

   b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with County policy and documented in the security plan for the information system.

   c. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.

   d. Maintain records for nonlocal maintenance and diagnostic activities.

   e. Terminate session and network connections when nonlocal maintenance is completed.

   f. Document in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

4. MAINTENANCE PERSONNEL
   County IT shall:

   a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

   b. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations.

   c. Designate County personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

5. TIMELY MAINTENANCE
   County IT shall:

   a. Obtain maintenance support and/or spare parts for information systems as agreed upon within the service level agreement between IT and the system owner.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
10.00	Media Protection Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) controls access to and disposes of media resources in compliance with County IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Media Protection (MP), NIST SP 800-12, NIST SP 800-56, NIST SP 800-57, NIST SP 800-60, NIST SP 800-88, NIST SP 800-100, NIST SP 800-111;
NIST Federal Information Processing Standards (FIPS) 199;
State of California State Administrative Manual (SAM) 5300 et seq**.,** Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. MEDIA ACCESS:
   County IT through direction from departments shall:

   a. Restrict access to ***digital and/or non-digital media*** to County IT staff and/or their designee.

   b. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.

2. MEDIA STORAGE
   County IT shall:

   a. Specify staff to physically control and securely store media within defined controlled areas.

   b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

3. MEDIA TRANSPORT
   County IT Shall:

   a. Protect and control media during transport outside of controlled areas.

   b. Maintain accountability for information system media during transport outside of controlled areas.

   c. Document activities associated with the transport of information system media.

   d. Restrict the activities associated with the transport of information system media to authorized personnel.

4. MEDIA SANITIZATION
   County IT shall:

   a. Sanitize prior to disposal, release out of organizational control, or release for reuse using media wiping tools and/or software in accordance with applicable federal and organizational standards and policies.

   b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

5. MEDIA USE
   County IT shall:

   Prohibit the use of County and Department defined types of information system media, such as USB drives, on County owned equipment using unapproved security safeguards where applicable.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
11.00	Physical and Environmental Protection Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Physical and Environmental Protection (PE), NIST SP 800-46, NIST SP 800-73, SP NIST 800-76, SP NIST 800-78, SP NIST 800-116;
Intelligence Community Directive (ICD): 704 705;
Department of Defense (DoD): Instruction 5200.39 Critical Program Information (CPI) Protection;
Federal Identity, Credential, and Access Management (FICAM) publication: Personal Identity Verification (PIV) in Enterprise Access Control System (E-PACS) (2012);
State of California: State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. PHYSICAL ACCESS AUTHORIZATIONS
   County IT shall:

   a. Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.

   b. Issue authorization credentials for facility access.

   c. Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.

2. PHYSICAL ACCESS CONTROL
   County IT shall:

   a. Enforce physical access authorizations by verifying individual access authorizations before granting access to the facility.

   b. Control ingress/egress to the facility using physical access control systems/devices and/or guards.

   c. Maintain physical access audit logs for County defined entry/exit points.

   d. Provide *security safeguards* to control access to areas within the facility officially designated as publicly accessible.

   e. Escort visitors and monitors visitor activity in *County specified areas*.

   f. Secure keys, combinations, and other physical access devices.

   g. Inventory County defined physical access devices every quarter or more frequently where required.

   h. Change combinations and keys *upon staff separation* and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

3. FACILITY PENETRATION TESTING
   County IT shall:

   a. Employ a penetration testing process that includes *annually* unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

4. ACCESS CONTROL FOR TRANSMISSION MEDIUM
   County IT shall:

   a. Control physical access to *information system distribution and transmission lines* within County facilities using *physical security safeguards*.

5. ACCESS CONTROL FOR OUTPUT DEVICES
   County IT shall:

   a. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

      Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by County personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

6. MONITORING PHYSICAL ACCESS
   County IT shall:

   a. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.

   b. Review physical access logs *monthly* and upon occurrence of potential violation of physical access; and coordinate results of reviews and investigations with the organizational incident response capability.

7. VISITOR ACCESS RECORDS
   County IT shall:

   a. Maintain visitor access records to the facility where the information system resides for *5* years; and reviews visitor access records *monthly*.

8. POWER EQUIPMENT AND CABLING
   County IT shall:

   a. Protect power equipment and power cabling for the information system from damage and destruction.

   b. Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

9. EMERGENCY SHUTOFF
   County IT shall:

   a. Provide the capability of shutting off power to the information system or individual system components in emergency situations.

b. Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorized activation.

10. EMERGENCY POWER
County IT shall:

a. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; transition of the information system to long-term alternate power in the event of a primary power source loss.

b. Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

11. EMERGENCY LIGHTING
County IT shall:

a. Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

b. Provide emergency lighting for all areas within the facility supporting essential missions and business functions.

12. FIRE PROTECTION
County IT shall:

a. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

13. TEMPERATURE AND HUMIDITY CONTROLS
County IT shall:

a. Maintain temperature and humidity levels within the facility where the information system resides at *County assigned data centers and/or data closets.*

b. Monitor temperature and humidity levels *continuously* to include alarms or notifications of changes potentially harmful to personnel or equipment.

14. WATER DAMAGE PROTECTION
County IT shall:

a. Protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

15. DELIVERY AND REMOVAL
    County IT shall:

    a. Authorize, monitor, and control entering and exiting the facility and maintain records of those items delivered and removed from facility.

       Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

16. ALTERNATE WORK SITE
    County IT shall:

    a. Employ *security controls* at alternate work sites when required to meet departmental standards.

    b. Assess as feasible, the effectiveness of security controls at alternate work sites.

    c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

       Alternate work sites may include, for example, other government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. County staff may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
12.00	County Planning Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Security Planning (PL), NIST SP 800-12, SP NIST 800-18,
NIST SP 800-100;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. SYSTEM SECURITY PLAN
   County IT shall:

   a. Develop a security plan for each information system that:

      i. Is consistent with the County's enterprise architecture.

      ii. Defines explicitly the authorization boundary for the system.

      iii. Describes the operational context of the information system in terms of missions and business processes.

      iv. Provides the security categorization of the information system including supporting rationale.

      v. Describes the operational environment for the information system and relationships with or connections to other information systems.

      vi. Provides an overview of the security requirements for the system.

      vii. Identifies any relevant overlays, if applicable.

      viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.

      ix. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

   b. Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel and/or business units.

   c. Review the security plan for the information system at least annually.

   d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

   e. Protect the security plan from unauthorized disclosure and modification.

2. RULES OF BEHAVIOR
   County IT shall:

   a. Establish, and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.

   b. Receive a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

   c. Review and update the rules of behavior.

   d. Require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised and updated.

3. INFORMATION SECURITY ARCHITECTURE
   County IT shall:

   a. Develop information security architecture for the information system that will:

      i. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.

      ii. Describe how the information security architecture is integrated into and supports the enterprise architecture.

      iii. Describe any information security assumptions and dependencies on external services.

   b. Review and update the information security architecture no less than annually, to reflect updates in the enterprise architecture.

   c. Ensure that planned information security architecture changes are reflected in the security plan, the security operations and County procurements/acquisitions.

4. DEFENSE-IN-DEPTH APPROACH
   County IT shall:

   a. Design security architecture using a defense-in-depth approach that:

      i. Allocates security safeguards to county defined locations and architectural layers.

      ii. Will ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation

measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
13.0	Personnel Security Policy	7/1/2017

PURPOSE

To ensure that personnel security safeguards are applied to the access and use of information technology resources and data.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Personnel Security (PS), NIST SP 800-12, NIST SP 800-60, NIST SP 800-73, NIST SP 800-78, NIST SP 800 -100;
Electronic Code of Federal Regulations (CFR): 5 CFR 731.106;
Federal Information Processing Standards (FIPS) 199 and 201;
Intelligence Community Directive (ICD) 704 Personnel Security Standards;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. POSITION RISK DESIGNATION
   County Information Technology (IT) shall:

   a. Assign a risk designation to all County positions.

   b. Establish screening criteria for individuals filling those positions.

   c. Review and update position risk designations ***annually***.

2. PERSONNEL SCREENING
   County IT and department system and application owners shall:

   a. Screen individuals prior to authorizing access to the information systems.

   b. Rescreen individuals according to ***defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening.***

   c. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

3. PERSONNEL TERMINATION
   County IT and departments shall, upon termination of individual employment:

   a. Disable information system access within ***the hour of notification of termination.***

   b. Terminate/revoke any authenticators/credentials associated with the individual.

   c. Conduct exit interviews that include a discussion of ***County defined information security topics.***

   d. Retrieve all security-related County information system-related property.

   e. Retain access to County information and information systems formerly controlled by terminated individual.

   f. Notify County IT and/or their designee within the hour.

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.

The County shall:

g. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of county information.

h. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the county termination process as directed by County Counsel and Human Resources (HR).

i. Employ automated mechanisms to notify *County IT and/or their designee* upon termination of an individual.

4. PERSONNEL TRANSFER
County IT and departments shall:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the County.

b. Initiate transfer or reassignment actions within 7 days following the formal transfer action.

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

d. Notify *County IT and their designee* within *7 days* of transfer.

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

5. ACCESS AGREEMENTS
County IT and departments shall:

a. Develop and document access agreements for County information systems.

b. Review and update the access agreements as defined within the agreement.

c. Ensure that individuals requiring access to County information and information systems:

i. Sign appropriate access agreements prior to being granted access.

ii. Re-sign access agreements to maintain access to County information systems when access agreements have been updated or *deemed necessary by the Department.*

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

6. THIRD-PARTY PERSONNEL SECURITY
County IT shall:

a. Establish and document personnel security requirements including security roles and responsibilities for third-party providers.

b. Require third-party providers to comply with personnel security policies and procedures established by the County.

c. Require third-party providers to notify *County IT and/or their designee* of any personnel transfers or terminations of third-party personnel who possess County credentials and/or badges, or who have information system privileges within *8 hours*.

d. Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

1. PERSONNEL SANCTIONS
County IT and County HR shall:

a. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures

b. Notify *County IT and/of their designee* within *24 hours* when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

County sanction processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organizations.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
14.0	Risk Assessment Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) performs risk assessments in compliance with County IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Risk Assessment (RA), NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NIST SP 800-60, NIST SP 800-70, NIST SP 800-100, NIST SP 800-115;
NIST Federal Information Processing Standards (FIPS) 199;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. SECURITY CATEGORIZATION
   County IT shall:

   a. Apply proper security controls to data categorized as confidential by system owners, including protected health information (PHI) and personally identifiable information (PII), in accordance with applicable federal and state laws, directives, policies, regulations, standards, and guidance.

   b. Document the security controls (including supporting rationale) in the security plan for the information system.

2. RISK ASSESSMENT
   County IT shall:

   a. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

   b. Document risk assessment results in annual IT Risk Assessment.

   c. Review risk assessment results quarterly.

   d. Disseminate risk assessment results to stakeholders.

   e. Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

3. VULNERABILITY SCANNING
   County IT shall:

   a. Scan for vulnerabilities in the information system and hosted applications weekly/monthly and/or randomly in accordance with the County IT incident policy and when new vulnerabilities potentially affecting the system/applications are identified and reported.

   b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

i. Enumerating platforms, software flaws, and improper configurations.

ii. Formatting checklists and test procedures.

iii. Measuring vulnerability impact.

c. Analyze vulnerability scan reports and results from security control assessments.

d. Remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.

e. Share information obtained from the vulnerability scanning process and security control assessments with the Chief Information Officer to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

f. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

g. Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported.

h. Ensure that information systems implement privileged access authorization to all systems for selected vulnerability scanning.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
15.0	County System and Services Acquisition Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) resources and information systems are acquired with security requirements to meet the County information systems mission and business objectives.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – System and Services Acquisition (SA), NIST SP 800-12, NIST SP 800-23, NIST SP 800-35, NIST SP 800-36, NIST SP 800-37, NIST SP 800-64, NIST SP 800-65, NIST SP 800-70, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137;
Homeland Security Presidential Directive (HSPD) 12;
International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) Standard 15408;
NIST Federal Information Processing Standards (FIPS) 140-2, FIPS 201;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. ALLOCATION OF RESOURCES
   County IT, in direct guidance and association with the County information system owner shall:

   a. Determine information security requirements for the information system or information system service in mission/business process planning.

   b. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process.

   c. Establish a discrete line item for information security in organizational programming and budgeting documentation.

2. SYSTEM DEVELOPMENT LIFE CYCLE
   County IT, in direct guidance and association with the County information system owner, shall develop a contingency plan for the information system that:

   a. Manages the information system using the County system development life cycle to ensure incorporation information security considerations.

   b. Defines and documents information security roles and responsibilities throughout the system development life cycle.

   c. Identifies individuals having information security roles and responsibilities.

   d. Integrates the information security risk management process into system development life cycle activities.

3. ACQUISITION PROCESS
   County IT shall ensure the acquisition process includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal, state, and local laws, Executive Orders, directives, policies, regulations, standards, guidelines, and County mission and business needs:

a. Security functional requirements.

b. Security strength requirements.

c. Security assurance requirements.

d. Security-related documentation requirements.

e. Requirements for protecting security-related documentation.

f. Description of the information system development environment and environment in which the system is intended to operate.

g. Acceptance criteria.

4. SECURITY CONTROLS
   County Information Technology (IT) shall require the information system, system component, or information system service:

   a. Describe the functional properties of the security controls to be employed; security-relevant external system interfaces; high-level design, low-level design, source code or hardware schematics that meet the business requirements.

   b. Identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

5. INFORMATION SYSTEM DOCUMENTATION
   County IT shall:

   a. Obtain administrator documentation for the information system, system component, or information system service that describes:

      i. Secure configuration, installation, and operation of the system, component, or service.

      ii. Effective use and maintenance of security functions/mechanisms.

      iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

   b. Obtain user documentation for the information system, system component, or information system service that describes:

      i. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.

      ii. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner.

      iii. User responsibilities in maintaining the security of the system, component, or service.

   c. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.

   d. Protect documentation as required, in accordance with the risk management strategy.

   e. Distribute documentation to only authorized persons or entities.

6. SECURITY ENGINEERING PRINCIPLES
   County IT shall:

   a. Apply industry standard information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

7. EXTERNAL INFORMATION SYSTEM SERVICES
   County IT shall:

   a. Require that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

   b. Define and document government oversight and user roles and responsibilities with regard to external information system services.

   c. Employ processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

   d. Require providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

8. DEVELOPER CONFIGURATION MANAGEMENT
   County IT shall ensure developers of the information system, system component, or information system service:

   a. Perform configuration management during system, component, or service design; development, implementation, and/or operation.

   b. Document, manage, and control the integrity of changes to configuration items under configuration management.

   c. Implement only organization-approved changes to the system, component, or service.

   d. Document approved changes to the system, component, or service and the potential security impacts of such changes.

   e. Track security flaws and flaw resolution within the system, component, or service and report findings to authorized personnel and/or business units.

9. DEVELOPER CONFIGURATION MANAGEMENT
   County IT shall:

   a. Require the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

   b. Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

   c. Require the developer of the information system, system component, or information system service to enable integrity verification of hardware components.

   d. Require the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.

   e. Require the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data

(hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

f. Require the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

10. DEVELOPER SECURITY TESTING AND EVALUATION
County IT shall require the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan.

b. Perform unit; integration; system; regression testing/evaluation.

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.

d. Implement a verifiable flaw remediation process.

e. Correct flaws identified during security testing/evaluation.

f. Employ static code analysis tools to identify common flaws and document the results of the analysis.

g. Perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

11. INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE
County IT shall:

a. Require an independent agent satisfying to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation.

b. Ensure that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.

c. Perform a manual code review of defined processes, procedures, and/or techniques.

d. Perform penetration testing.

e. Verify that the scope of security testing/evaluation provides complete coverage of required security controls.

f. Employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
16.0	County System and Communications Protection Policy	07/01/2017

PURPOSE

To establish guidelines for system and communications protection for County Information Technology (IT) resources and information systems.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-53a - System and Communications Protection (SC), NIST SP 800-12, NIST SP 800-28, NIST SP 800-41, NIST SP 800-52, NIST SP 800-56, NIST SP 800-57, NIST SP 800-58, NIST SP 800-77, NIST SP 800-81, NIST SP 800-95, NIST SP 800-100, NIST SP 800-111, NIST SP 800-113;
NIST Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 199; State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. APPLICATION PARTITIONING
   County IT shall:

   a. Separate user functionality from information system management functionality either logically or physically.

      Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.

2. INFORMATION IN SHARED RESOURCES
   County IT shall:

   a. Prevent unauthorized and unintended information transfer via shared system resources.

      This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

3. DENIAL OF SERVICE PROTECTION
   County IT shall:

   a. Ensure that the information system protects against or limits the effects of denial of service attacks.
   b. The information system restricts the ability of individuals to launch denial of service attacks against other information systems.

4. BOUNDARY PROTECTION
   County IT shall:

   a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

   b. Implement sub-networks for publicly accessible system components that are [physically; logically] separated from internal organizational networks, and connected to external

networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within security architecture.

5. TRANSMISSION CONFIDENTIALITY AND INTEGRITY
   County IT shall:

   a. Deploy information systems that protect the [confidentiality; integrity] of transmitted information.

      This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

6. NETWORK DISCONNECT
   On Departmental specified network segments, County IT shall:

   a. Ensure information systems are configured to terminate the network connection associated with a communications session at the end of the session or after *30 days* of inactivity; this control applies to both internal and external networks.

      Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

7. CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
   County IT shall:

   a. Establish and manage cryptographic keys for required cryptography employed within the information system in accordance with County defined requirements for key generation, distribution, storage, access, and destruction.

8. CRYPTOGRAPHIC PROTECTION
   County IT shall:

   a. Implement County defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal and state laws, directives, policies, regulations, and standards.

      Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.

9. COLLABORATIVE COMPUTING DEVICES
   County IT shall:

   a. Prohibit remote activation of collaborative computing devices with the following exceptions: County defined exceptions where remote activation is to be allowed.

   b. Provide an explicit indication of use to users physically present at the devices.

      Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

10. PUBLIC KEY INFRASTRUCTURE CERTIFICATES
    County IT shall:

    a. Issue public key certificates under a [defined certificate policy] or obtain public key certificates from an approved service provider.

    b. Manage information system trust stores for all key certificates to ensure only approved trust anchors are in the trust stores.

11. MOBILE CODE
    County IT shall:

    a. Define acceptable and unacceptable mobile code and mobile code technologies.

    b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

    c. Authorize, monitor, and control the use of mobile code within the information system.

       Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.

12. VOICE OVER INTERNET PROTOCOL
    County IT shall:

    a. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

    b. Authorize, monitor, and control the use of VoIP within the information system.

13. SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
    County IT shall:

    a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

    b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

       This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

14. SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
    County IT shall:

    a. Ensure information systems that requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

       Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

15. ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
    County IT shall:

    a. Ensure the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

    b. Employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server, to eliminate single points of failure and to enhance redundancy.

       Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.

16. SESSION AUTHENTICITY
    County IT shall:

    a. Ensure the information system protects the authenticity of communications sessions.

       This control addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

17. PROTECTION OF INFORMATION AT REST
    County IT shall:

    a. Ensure the information system protects the confidentiality/integrity of County defined information at rest.

       This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

18. PROCESS ISOLATION
    County IT shall:

    a. Ensure the information system maintains a separate execution domain for each executing process.

       Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for

achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Policy #:	Title:	Effective Date:
17.0	County System and Information Integrity Policy	07/01/2017

PURPOSE

To ensure that County Information Technology (IT) resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – System and Information Integrity (SI), NIST SP 800-12, NIST SP 800-40, NIST SP 800-45, NIST SP 800-83, NIST SP 800-61, NIST SP800-83, NIST SP 800-92, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137, NIST SP 800-147, NIST SP 800-155;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. FLAW REMEDIATION
   County IT shall:

   a. Identify, report, and correct information system flaws.

   b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

   c. Install security-relevant software and firmware updates within 7 days of the release of the updates.

   d. Incorporate flaw remediation into the County configuration management process.

   e. Employ automated mechanisms nightly reports to determine the state of information system components with regard to flaw remediation.

2. MALICIOUS CODE PROTECTION
   County IT shall:

   a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

   b. Update malicious code protection mechanisms whenever new releases are available in accordance with County configuration management policy and procedures.

   c. Configure malicious code protection mechanisms to:

      i. Perform periodic scans of the information system daily and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with county security policy.

      ii. Block malicious code; quarantine malicious code; send alert to administrator; immediately in response to malicious code detection.

      iii. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

1. INFORMATION SYSTEM MONITORING
   County IT shall:

   a. Monitor the information system to detect:

      i. Attacks and indicators of potential attacks.

      ii. Unauthorized local, network, and remote connections.

   b. Identify unauthorized use of the information system through defined techniques and methods.

   c. Deploy monitoring devices strategically within the information system to collect accidental transmission of Personally Identifiable Information and at ad hoc locations within the system to track specific types of transactions of interest to the County.

   d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

   e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to County operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.

   f. Obtain legal counsel with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.

   g. Provide information system monitoring information to authorized personnel or business units as needed.

2. SYSTEM-GENERATED ALERTS
   County IT shall ensure that:

   a. The system generated alerts that may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers will be disseminated to authorized personnel or business units that shall take appropriate action on the alert(s).

   b. Alerts be transmitted telephonically, electronic mail messages, or by text messaging as required. County personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.

3. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
   County IT shall:

   a. Receive information system security alerts, advisories, and directives from MS-ISAC Security Advisory and Homeland Security Information Network on an ongoing basis.

   b. Generate internal security alerts, advisories, and directives as deemed necessary throughout the County.

   c. Disseminate security alerts, advisories, and directives to:
      - Information Services Manager
      - Information Security Officer
      - Network Systems and Support Supervising Analysts
      - Network Systems and Support Analysts

   d. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

4. SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
   County IT shall:

   a. Employ integrity verification tools to detect unauthorized changes to systems in the following categories:

Workstations Operating Systems	Workstations Software
Server Operating Systems	Server Software
All Network Equipment	

   b. Ensure the information system performs an integrity check of aforementioned items at startup, and/or at County defined transitional states or security-relevant events.

   c. Incorporate the detection of unauthorized software installation into the County incident response capability.

5. SPAM PROTECTION
   County IT shall:

   a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.

   b. Update spam protection mechanisms when new releases are available in accordance with County configuration management policy and procedures.

   c. Manage spam protection mechanisms centrally.

   d. Ensure information systems automatically update spam protection mechanisms.

6. INFORMATION HANDLING AND RETENTION
   County IT shall:

   a. Handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Policy #:	Title:	Effective Date:
18.0	Countywide Computer Security Threat Response Policy	07/01/2017

PURPOSE

The purpose of this policy is to define the County's responsibility in responding to security threats affecting the confidentiality, integrity, and/or availability of County information technology (IT) resources.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-61 - Computer Security Incident Handling Guide;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

POLICY

This policy is applicable to all County departments and all County information systems.

1. COUNTYWIDE COMPUTER EMERGENCY RESPONSE

    a. The County shall establish a Countywide Computer Emergency Response Team (CCERT). The CCERT shall be led by the Chief Information Officer or their equivalent when the CIO is not available.

    b. The CCERT shall consist of representatives from all County departments.

    c. The CCERT shall communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate, or eliminate security threats to County IT resources.

    d. Upon the activation of CCERT by the CIO or designated IT staff, all Departmental Information Security Officers (DISOs), Assistant DISOs, and other CCERT representatives shall report directly to the CHIEF INFORMATION OFFICER (CIO) OR DESIGNATED IT STAFF for the duration of the CCERT activation.

2. DEPARTMENTAL COMPUTER EMERGENCY RESPONSE

    a. Each County department shall establish a Departmental Computer Emergency Response Team (DCERT) that is led by the DISO and has the responsibility for responding to and/or coordinating the response to security threats to County IT resources within the County department.

    b. Representatives from each DCERT shall also be active participants in CCERT.

    c. Upon the activation of a County department's DCERT by the DISO, all DCERT representatives shall report directly to the DISO for the duration of the DCERT activation.

    d. Each County department shall establish and implement Departmental Computer Emergency Response Procedures that consist of the following, at minimum:

        i. Creating an incident response policy and plan.

        ii. Developing procedures for performing incident handling and reporting.

        iii. Setting guidelines for communicating with outside parties regarding incidents.

        iv. Selecting a team structure and staffing mode.

v. Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies.

vi. Determining what services the incident response team should provide.

vii. Staffing and training the incident response team.

e. The DCERT shall inform the CCERT, as early as possible, of security threats to County IT resources.

f. Each County department shall develop a notification process, to ensure management notification within the County department and to the CCERT, in response to County IT security incidents.

g. The CCERT and DCERTs have the responsibility to take necessary corrective action to remediate County IT security incidents. Such action shall include all necessary steps to preserve evidence in order to facilitate the discovery, investigation, and prosecution of crimes against County IT resources.

h. Each County department shall provide CCERT with contact information, including, without limitation, after-hours, for its primary and secondary CCERT representatives (e.g., DISO and Assistant DISO), and immediately notify CCERT of any changes to that information.

i. Each County department shall maintain current contact information for all personnel who are important for the response to security threats to County IT resources and/or the remediation of County IT security incidents.

j. Each County department shall provide its primary and secondary CCERT representatives with adequate portable communication devices (e.g., cell phone and pager).

k. In instances where violation of any law may have occurred, proper notifications shall be made in accordance with County policies. All necessary action shall be taken to preserve evidence and facilitate the administration of justice.

3. DEFINITION REFERENCE

a. As used in this policy, the term “County IT resources” shall have the same meaning as the definition established in the County Information Security Program.

b. As used in this policy, the term “County IT security” shall have the same meaning as the definition established in the County Information Security Program.

c. As used in this policy, the term “County IT security incident” shall have the same meaning as the definition established in the County Information Security Program.

d. As used in this policy, the term “County department” shall have the same meaning as the definition established in the County Information Security Program.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or designated IT staff. Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

RESPONSIBLE DEPARTMENT

Chief Information Office and County Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	07/01/2017
Date Reviewed:	07/01/2021

Appendix A: Glossary

COMMON TERMS AND DEFINITIONS

Appendix A provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Adequate Security [OMB Circular A-130, Appendix III, Adapted]	Security commensurate with the risk resulting from the loss, misuse, or unauthorized access to or modification of information.
Advanced Persistent Threat	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.
Agency	See *Executive Agency*.
All Source Intelligence [Department of Defense, Joint Publication 1-02]	Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence.
Assessment	See *Security Control Assessment*.
Assessor	See *Security Control Assessor*.
Assurance [CNSSI 4009]	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.
Assurance Case [Software Engineering Institute, Carnegie Mellon University]	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.
Audit Log [CNSSI 4009]	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Record	An individual entry in an audit log related to an audited event.
Audit Reduction Tools [CNSSI 4009]	Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups.
Audit Trail [CNSSI 4009]	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).

Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See *Authentication*.
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorize Processing	See *Authorization*.
Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
Blacklisting	The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) prohibited Universal Resource Locators (URL)/websites.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).
Boundary Protection Device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.
Central Management	The organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes.
Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. Note: Organizations subordinate to federal agencies may use the term *Chief Information Officer* to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.

Chief Information Security Officer	See *Senior Agency Information Security Officer*.
Chief Privacy Officer	See *Senior Agency Official for Privacy*.
Classified Information	Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD).
Commodity Service	An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.
Common Carrier	In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions.
Common Control [NIST SP 800-37; CNSSI 4009]	A security control that is inheritable by one or more organizational information systems. See *Security Control Inheritance*.
Common Control Provider [NIST SP 800-37]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inheritable by information systems).
Common Criteria [CNSSI 4009]	Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.
Common Secure Configuration	A recognized standardized and established benchmark that stipulates specific secure configuration settings for a given information technology platform.
Compensating Security Controls [CNSSI 4009, Adapted]	The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.
Computer Matching Agreement	An agreement entered into by an organization in connection with a computer matching program to which the organization is a party, as required by the Computer Matching and Privacy Protection Act of 1988. With certain exceptions, a computer matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSSI 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Configuration Item	An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.
Controlled Area	Any area or space for which an organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
Controlled Interface [CNSSI 4009]	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.
Controlled Unclassified Information [E.O. 13556]	A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.
Countermeasures [CNSSI 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Covert Channel Analysis [CNSSI 4009]	Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.
Covert Storage Channel [CNSSI 4009]	Covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.
Covert Timing Channel [CNSSI 4009]	Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.
Cross Domain Solution [CNSSI 4009]	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
Cyber Attack [CNSSI 4009]	An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber Security [CNSSI 4009]	The ability to protect or defend the use of cyberspace from cyber attacks.
Cyberspace [CNSSI 4009]	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Data Mining/Harvesting	An analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery.

Defense-in-Breadth [CNSSI 4009]	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Developer	A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form.
Discretionary Access Control [CNSSI 4009]	An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability. A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).
Domain [CNSSI 4009]	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See *Security Domain*.
Enterprise [CNSSI 4009]	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See *Organization*.
Enterprise Architecture [44 U.S.C. Sec. 3601]	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information system processes, stores, and transmits information.
Event [CNSSI 4009, Adapted]	Any observable occurrence in an information system.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

Exfiltration	The unauthorized transfer of information from an information system.
External Information System (or Component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
External Network	A network not controlled by the organization.
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.
Fair Information Practice Principles	Principles that are widely accepted in the United States and internationally as a general framework for privacy and that are reflected in various federal and international laws and policies. In a number of organizations, the principles serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies.
Federal Agency	See *Executive Agency*.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for government wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
FIPS-Validated Cryptography	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-Approved Cryptography*.
Firmware [CNSSI 4009]	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
Guard (System) [CNSSI 4009, Adapted]	A mechanism limiting the exchange of information between information systems or subsystems.
Hardware [CNSSI 4009]	The physical components of an information system. See *Software* and *Firmware*.
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high.

Hybrid Security Control [CNSSI 4009]	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.
Impact Value	The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.
Incident [FIPS 200]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.
Information [CNSSI 4009] [FIPS 199]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. An instance of an information type.
Information Leakage	The intentional or unintentional release of information to an untrusted environment.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise’s security processes, information security systems, personnel and organizational subunits, showing their alignment with the enterprise’s mission and strategic plans.
Information Security Policy [CNSSI 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Information Steward [CNSSI 4009]	An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
Information System Boundary	See *Authorization Boundary*.
Information System Component [NIST SP 800-128, Adapted]	A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Resilience	The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.
Information System Security Officer [CNSSI 4009]	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
Information System Service	A capability provided by an information system that facilitates information processing, storage, or transmission.
Information System-Related Security Risks	Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *Risk*.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Technology Product	See *Information System Component*.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Insider [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	Any person with authorized access to any U.S. Government resource, to include personnel, facilities, information, equipment, networks, or systems.

Insider Threat [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
[CNSSI 4009]	An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.
Insider Threat Program [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	A coordinated group of capabilities under centralized management that is organized to detect and prevent the unauthorized disclosure of sensitive information. At a minimum, for departments and agencies that handle classified information, an insider threat program shall consist of capabilities that provide access to information; centralized information integration, analysis, and response; employee insider threat awareness training; and the monitoring of user activity on government computers. For department and agencies that do not handle classified information, these can be employed effectively for safeguarding information that is unclassified but sensitive.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Internal Network	A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
Label	See *Security Label*.
Line of Business	The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.
Local Access	Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
Logical Access Control System [FICAM Roadmap and Implementation Guidance]	An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Malware	See *Malicious Code*.
Managed Interface	An interface within an information system that provides boundary protection capability using automated mechanisms or devices.

Mandatory Access Control [CNSSI 4009]	An access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly-created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints. A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. Mandatory Access Control is a type of nondiscretionary access control.
Marking	See *Security Marking*.
Media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Metadata	Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a FIPS Publication 199 potential impact value of high.
Multifactor Authentication	Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See *Authenticator*.
Multilevel Security [CNSSI 4009]	Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.

Multiple Security Levels [CNSSI 4009]	Capability of an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security domains.
National Security Emergency Preparedness Telecommunications Services [47 C.F.R., Part 64, App A]	Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Network [CNSSI 4009]	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Network Access	Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
Nondiscretionary Access Control	See *Mandatory Access Control*.
Nonlocal Maintenance	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.
Non-Organizational User	A user who is not an organizational user (including public users).
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
NSA-Approved Cryptography	Cryptography that consists of: (i) an approved algorithm; (ii) an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a particular environment; and (iii) a supporting key management infrastructure.
Object	Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See *Subject*.
Operations Security [CNSSI 4009]	Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).
Organizational User	An organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.
Overlay	A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.
Penetration Testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
Personally Identifiable Information [OMB Memorandum 07-16]	Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).
Physical Access Control System [FICAM Roadmap and Implementation Guidance]	An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Portable Storage Device	An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
Privacy Act Statement	A disclosure statement required by Section (e)(3) of the Privacy Act of 1974, as amended, to appear on documents used by organizations to collect personally identifiable information from individuals to be maintained in a Privacy Act System of Records (SORN).
Privacy Impact Assessment [OMB Memorandum 03-22]	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged Account	An information system account with authorizations of a privileged user.

Privileged Command	A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.
Privileged User [CNSSI 4009]	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Provenance	The records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes. Provenance enables all changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities.
Public Key Infrastructure [CNSSI 4009]	The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.
Purge	Rendering sanitized data unrecoverable by laboratory attack methods.
Reciprocity [CNSSI 4009]	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Red Team Exercise	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.
Reference Monitor	A set of design requirements on a reference validation mechanism which as key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism must be: (i) always invoked (i.e., complete mediation); (ii) tamperproof; and (iii) small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable).
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
Remote Maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
Resilience	See *Information System Resilience*.

Restricted Data [Atomic Energy Act of 1954]	All data concerning (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 [of the Atomic Energy Act of 1954].
Risk [FIPS 200, Adapted]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Executive (Function) [CNSSI 4009]	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management [CNSSI 4009, adapted]	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Mitigation [CNSSI 4009]	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
Risk Monitoring	Maintaining ongoing awareness of an organization’s risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
Role-Based Access Control	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Safeguards [CNSSI 4009]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Scoping Considerations	A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective.
Security [CNSSI 4009]	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
Security Assessment	See *Security Control Assessment*.
Security Assessment Plan	The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment.
Security Assurance	See *Assurance*.
Security Attribute	An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system and used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.
Security Authorization	See *Authorization*.
Security Authorization Boundary	See *Authorization Boundary*.
Security Capability	A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See *Security Category*.
Security Category [FIPS 199, Adapted; CNSSI 4009]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

Security Control [FIPS 199, Adapted]	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Control Assessment [CNSSI 4009, Adapted]	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline [FIPS 200, Adapted]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.
Security Control Enhancement	Augmentation of a security control to: (i) build in additional, but related, functionality to the control; (ii) increase the strength of the control; or (iii) add assurance to the control.
Security Control Inheritance [CNSSI 4009]	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.
Security Control Overlay	See *Overlay*.
Security Domain [CNSSI 4009]	A domain that implements a security policy and is administered by a single authority.
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis [CNSSI 4009]	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Incident	See *Incident*.
Security Kernel [CNSSI 4009]	Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct.
Security Label	The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.
Security Marking	The means used to associate a set of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.
Security Policy [CNSSI 4009]	A set of criteria for the provision of security services.

Security Policy Filter	A hardware and/or software component that performs one or more of the following functions: (i) content verification to ensure the data type of the submitted content; (ii) content inspection, analyzing the submitted content to verify it complies with a defined policy (e.g., allowed vs. disallowed file constructs and content portions); (iii) malicious content checker that evaluates the content for malicious code; (iv) suspicious activity checker that evaluates or executes the content in a safe manner, such as in a sandbox/detonation chamber and monitors for suspicious activity; or (v) content sanitization, cleansing, and transformation, which modifies the submitted content to comply with a defined policy.
Security Requirement [FIPS 200, Adapted]	A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.
Security Service [CNSSI 4009]	A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.
Security-Relevant Information	Any information within the information system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.
Senior Agency Official for Privacy	The senior organizational official with overall organization-wide responsibility for information privacy issues.
Senior Information Security Officer	See *Senior Agency Information Security Officer*.
Sensitive Information [CNSSI 4009, Adapted]	Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Sensitive Compartmented Information [CNSSI 4009]	Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.
Service-Oriented Architecture	A set of principles and methodologies for designing and developing software in the form of interoperable services. These services are well-defined business functions that are built as software components (i.e., discrete pieces of code and/or data structures) that can be reused for different purposes.
Software [CNSSI 4009]	Computer programs and associated data that may be dynamically written or modified during execution.

Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Special Access Program [CNSSI 4009]	A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Subject	Generally an individual, process, or device causing information to flow among objects or change to the system state. See *Object*.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplemental Guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
Supplementation	The process of adding security controls or control enhancements to a security control baseline as part of the tailoring process (during security control selection) in order to adequately meet the organization's risk management needs.
Supply Chain [ISO 28001, Adapted]	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Supply Chain Element	An information technology product or product component that contains programmable logic and that is critically important to the functioning of an information system.
System	See *Information System*.
System of Records Notice	An official public notice of an organization's system(s) of records, as required by the Privacy Act of 1974, that identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system of records; (iii) the categories of records maintained about individuals; and (iv) the ways in which the information is shared.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to a security control baseline. See *Tailoring*.
Tailoring	The process by which security control baselines are modified by: (i) identifying and designating common controls; (ii) applying scoping considerations on the applicability and implementation of baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to organization-defined security control parameters; (v) supplementing baselines with additional security controls or control enhancements; and (vi) providing additional specification information for control implementation.
Threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Assessment [CNSSI 4009]	Formal description and evaluation of threat to an information system.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
Trustworthiness [CNSSI 4009]	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.
Trustworthiness (Information System)	The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.
User [CNSSI 4009, adapted]	Individual, or (system) process acting on behalf of an individual, authorized to access an information system. See *Organizational User* and *Non-Organizational User*.
Virtual Private Network [CNSSI 4009]	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Analysis	See *Vulnerability Assessment*.
Vulnerability Assessment [CNSSI 4009]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
Whitelisting	The process used to identify: (i) software programs that are authorized to execute on an information system; or (ii) authorized Universal Resource Locators (URL)/websites.

Appendix B: Acronyms

COMMON ABBREVIATIONS

APT	Advanced Persistent Threat
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
DCS	Distributed Control System
DNS	Domain Name System
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITL	Information Technology Laboratory
LACS	Logical Access Control System
LSI	Large-Scale Integration
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information System Security Instruction
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPSEC	Operations Security
PBX	Private Branch Exchange
PACS	Physical Access Control System
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RD	Restricted Data

RMF	Risk Management Framework
SAISO	Senior Agency Information Security Officer
SAMI	Sources And Methods Information
SAOP	Senior Agency Official for Privacy
SAP	Special Access Program
SC	Security Category
SCADA	Supervisory Control and Data Acquisition
SCI	Sensitive Compartmented Information
SOA	Service-Oriented Architecture
SORN	System of Records Notice
SP	Special Publication
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

California County Information Services Directors Association

California Counties IT Policies for the Countywide

Information Security Program

Appendix C: Security and Privacy Control Catalog Compliance Mapping

CCISDA Information Security Forum
April 2016

Appendix C: Security and Privacy Control Catalog Compliance Mapping

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
Access Control Family							
AC-1	Access Control Policy and Procedures		5360 Identity and Access Management	Critical Control 15: Controlled Access Based on the Need to Know	9.3.1.1 Access Control Policy and Procedures	164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C, 164.312(a)(1)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.1.1, A.11.3.3, A.11.4.1, A.11.6.1, A.11.7.1, A.11.7.2, A.12.3.2, A.15.1.1, A.15.2.1
AC-2	Account Management		5315.8 Information Asset Connections 5335 Information Security Monitoring 5360 Identity and Access Management	"Critical Control 15: Controlled Access Based on the Need to Know	9.3.1.2 Account Management	164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C, 164.308(a)(5)(ii)(C, 164.312(a)(2)(i), 164.312(a)(2)(ii)	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A.11.5.2, A.11.5.5, A.11.5.6

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AC-3	Access Enforcement		5350.1 Encryption 5360 Identity and Access Management	"Critical Control 15: Controlled Access Based on the Need to Know	9.3.1.3 Access Enforcement	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C, 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)	A.7.2.2, A.10.6.1, A.10.7.3, A.10.7.4, A.10.8.1 A.10.9.1, A.10.9.2, A.10.9.3, A.11.2.2, A.11.5.4, A.11.6.1, A.12.4.3, A.15.1.3
AC-4	Information Flow Enforcement		5315.8 Information Asset Connections 5360 Identity and Access Management	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 15: Controlled Access Based on the Need to Know. Critical Control 17: Data Loss Prevention	9.3.1.4 Information Flow Enforcement	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.310(b)	A.7.2.2, A.10.7.3, A.10.8.1, A.11.4.5, A.11.4.7, A.12.5.4
AC-5	Separation of Duties		5360 Identity and Access Management		9.3.1.5 Separation of Duties	164.308(a)(3)(i), 164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.312(a)(1)	A.10.1.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AC-6	Least Privilege		5360 Identity and Access Management	Critical Control 12: Controlled Use of Administrative Privileges Critical Control 15: Controlled Access Based on the Need to Know	9.3.1.6 Least Privilege	164.308(a)(3)(i), 164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.312(a)(1)	A.11.2.2, A.11.4.1, A.11.4.4, A.11.5.4, A.11.6.1, A.12.4.3
AC-7	Unsuccessful Logon Attempts		5335 Information Security Monitoring 5335.2 Auditable Events 5360 Identity and Access Management		9.3.1.7 Unsuccessful Logon Attempts		A.11.5.1
AC-8	System Use Notification		5360 Identity and Access Management	9.3.1.8 System Use Notification			A.6.2.2, A.11.5.1, A.15.1.5
AC-11	Session Lock		5360 Identity and Access Management		9.3.1.9 Session Lock	164.310(b), 164.312(a)(2)(iii)	A.11.3.2, A.11.3.3, A.11.5.5
AC-12	Session Termination		5360 Identity and Access Management		9.3.1.10 Session Termination	164.310(b), 164.312(a)(2)(iii)	A.11.5.5
AC-14	Permitted Actions without Identification or Authentication		5360 Identity and Access Management		9.3.1.11 Permitted Actions without Identification or Authentication	164.312(a)(2)(ii)	None

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AC-17	Remote Access		5315.8 Information Asset Connections 5360 Identity and Access Management 5360.1 Remote Access	Critical Control 7: Wireless Device Control. Critical Control 12: Controlled Use of Administrative Privileges. Critical Control 13: Boundary Defense. Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.1.12 Remote Access 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.7 Telework Locations)	164.310(b)	A.10.6.1, A.10.8.1, A.10.8.5, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1, A.11.7.2
AC-18	Wireless Access		5315.8 Information Asset Connections 5360 Identity and Access Management 5360.2 Wireless Access	Critical Control 7: Wireless Device Control	9.3.1.13 Wireless Access		A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1
AC-19	Access Control for Mobile Devices		5315.8 Information Asset Connections 5360 Identity and Access Management	Critical Control 12: Controlled Use of Administrative Privileges. Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.1.14 Access Control for Mobile Devices	164.310(b)	A.9.2.5, A.10.4.1, A.10.7.3, A.11.4.3, A.11.4.6, A.11.7.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AC-20	Use of External Information Systems		5315.8 Information Asset Connections 5360 Identity and Access Management	Critical Control 13: Boundary Defense	9.3.1.15 Use of External Information Systems		A.6.2.1, A.7.1.3, A.9.2.5, A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6
AC-21	Information Sharing		5315.8 Information Asset Connections 5360 Identity and Access Management		9.3.1.16 Information Sharing Restricting Access—IRC 6103(p)(4)(C); (5.4 Controls over Processing)		None
AC-22	Publicly Accessible Content		5310 Privacy		9.3.1.17 Publicly Accessible Content		A.10.9.3, A.11.6.1
Audit and Accountability Family							
AU-1	Audit and Accountability Policy and Procedures		5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.1 Audit and Accountability Policy and Procedures 3.0 Record Keeping Requirement (3.1 General)	164.312(b)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1, A.15.3.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AU-2	Audit Events		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 12: Controlled Use of Administrative Privileges. Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.3 Audit Events 3.0 Record Keeping Requirement (3.2 Electronic and Non-Electronic FTI Logs)	164.308(a)(5)(ii)(C, 164.312(b)	A.10.10.1, A.10.10.2, A.10.10.4, A.10.10.5, A.11.5.4, A.15.3.1
AU-3	Content of Audit Records		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.4 Content of Audit Records 3.0 Record Keeping Requirement (3.2 Electronic and Non-Electronic FTI Logs)	164.312(b)	A.10.10.1, A.10.10.2, A.10.10.4
AU-4	Audit Storage Capacity		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.5 Audit Storage Capacity	164.312(b)	A.10.3.1, A.10.10.3
AU-5	Response to Audit Processing Failures		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.6 Response to Audit Processing Failures	164.312(b)	A.10.3.1, A.10.10.3
AU-6	Audit Review, Analysis, and Reporting		5335 Information Security Monitoring 5335.1 Continuous Monitoring	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.7 Audit Review, Analysis, and Reporting	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C, 164.312(b)	A.10.10.2, A.10.10.5, A.13.1.1, A.15.1.5

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AU-7	Audit Reduction and Report Generation		5335 Information Security Monitoring 5335.1 Continuous Monitoring		9.3.3.8 Audit Reduction and Report Generation	164.308(a)(1)(ii)(D), 164.312(b)	A.10.10.2, A.13.2.3
AU-8	Time Stamps		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.9 Time Stamps		A.10.10.1, A.10.10.6, A.13.2.3
AU-9	Protection of Audit Information		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.10 Protection of Audit Information		A.10.10.3, A.13.2.3, A.15.1.3, A.15.3.2
AU-11	Audit Record Retention		5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.11 Audit Record Retention (AU-11) 8.0 Disposing of FTI—IRC 6103(p)(4)(F); (General 8.1)	164.316(b)(1), 164.316(b)(2)(i)	A.10.10.1, A.13.2.3, A.15.1.3
AU-12	Audit Generation		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.12 Audit Generation		A.10.10.1, A.10.10.2, A.10.10.4, A.10.10.5
Security Assessment and Authorization Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CA-3	System Interconnections		5305.8 Provisions for Agreements with State and Non-State Entities	Critical Control 13: Boundary Defense	9.3.4.3 System Interconnections	164.308(b)(1), 164.308(b)(4), 164.314(a)(2)(ii)	A.6.2.1, A.6.2.2, A.6.2.3, A.10.6.1, A.10.6.2, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2
CA-5	Plan of Action and Milestones		5300.5 Minimum Security Controls 5330 Information Security Compliance 5330.1 Security Assessments		9.3.4.4 Plan of Action and Milestones 6.0 Other Safeguards—IRC 6103(p)(4)(D);(6.5 Plan of Action and Milestones)	164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(C)	None
CA-6	Security Authorization		5305.8 Provisions for Agreements with State and Non-State Entities 5315.8 Information Asset Connections 5360 Identity and Access Management		9.3.4.5 Security Authorization	164.308(a)(2), 164.308(a)(8)	A.6.1.4, A.10.3.2
CA-7	Continuous Monitoring		5300.5 Minimum Security Controls 5330 Information Security Compliance 5330.1 Security Assessments	Critical Control 20: Penetration Tests and Red Team Exercises	9.3.4.6 Continuous Monitoring	164.308(a)(1)(ii)(D), 164.308(a)(8)	A.6.1.8, A.12.6.1, A.13.1.2, A.15.2.1, A.15.2.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CA-9	Internal System Connections		5315.8 Information Asset Connections 5360 Identity and Access Management				None
Configuration Management Family							
CM-1	Configuration Management Policy and Procedures		5315.3 Configuration Management	Critical Control 2: Inventory of Authorized and Unauthorized Software. Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.	9.3.5.1 Configuration Management Policy and Procedures		A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-2	Baseline Configuration		5315.6 Activate only Essential Functionality	Critical Control 2: Inventory of Authorized and Unauthorized Software. Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.	9.3.5.2 Baseline Configuration		A.10.1.2, A.10.1.4, A.12.4.1
CM-3	Configuration Change Control		5315.3 Configuration Management	Critical Control 2: Inventory of Authorized and Unauthorized Software. Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.	9.3.5.3 Configuration Change Control		A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-4	Security Impact Analysis		5315 Information Security Integration 5315.3 Configuration Management		9.3.5.4 Security Impact Analysis		A.10.1.2, A.10.1.4, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3
CM-5	Access Restrictions for Change		5315.3 Configuration Management	Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 3: Secure Configurations for Hardware and Software Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	9.3.5.5 Access Restrictions for Change		A.10.1.2, A.12.4.1, A.12.4.3, A.12.5.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-6	Configuration Settings		5315.6 Activate only Essential Functionality	Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	9.3.5.6 Configuration Settings		A.10.10.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-7	Least Functionality		5315.6 Activate Only Essential Functionality	Critical Control 2: Inventory of Authorized and Unauthorized Software. Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches Critical Control 6: Application Software Security. Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	9.3.5.7 Least Functionality		A.11.4.1, A.11.4.4, A.11.4.6, A.12.4.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-8	Information System Component Inventory		5305.5 Information Asset Management	Critical Control 1: Inventory of Authorized and Unauthorized Devices Critical Control 2: Inventory of Authorized and Unauthorized Software	9.3.5.8 Information System Component Inventory	164.310(d)(1), 164.310(d)(2)(iii)	A.7.1.1, A.7.1.2
CM-9	Configuration Management Plan		5315.3 Configuration Management	Critical Control 2: Inventory of Authorized and Unauthorized Software	9.3.5.9 Configuration Management Plan		A.6.1.3. A.7.1.1, A.7.1.2, A.10.1.2, A.10.1.4, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3
CM-10	Software Usage Restrictions		5315.7 Software Usage Restrictions		9.3.5.10 Software Usage Restrictions		A.12.4.1, A.15.1.2
CM-11	User-Installed Software		5315.7 Software Usage Restrictions		9.3.5.11 User-Installed Software		A.10.4.1, A.10.10.2, A.12.4.1, A.15.1.5
Contingency Planning Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CP-2	Contingency Plan		5325 Business Continuity with Technology Recovery		9.3.6.2 Contingency Plan	164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C, 164.308(a)(7)(ii)(E, 164.310(a)(2)(i), 164.312(a)(2)(ii)	A.6.1.2, A.6.1.3, A.9.1.4, A.10.3.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.1.4, A.14.1.5
CP-3	Contingency Training		5325 Business Continuity with Technology Recovery 5325.2 Technology Recovery Training		9.3.6.3 Contingency Training	164.308(a)(7)(ii)(D)	A.8.2.2
CP-4	Contingency Plan Testing		5325 Business Continuity with Technology Recovery 5325.3 Technology Recovery Testing		9.3.6.4 Contingency Plan Testing	164.308(a)(7)(ii)(D)	A.6.1.2, A.14.1.4, A.14.1.5
CP-6	Alternate Storage Site		5305.8 Provisions for Agreements with State and Non-State Entities 5325.4 Alternate Storage and Processing Site		9.3.6.5 Alternate Storage Site Restricting Access—IRC 6103(p)(4)(C); (5.4.2 Contractor- or Agency-Shared Facility—Consolidated Data Centers)	164.308(a)(7)(ii)(B), 164.310(a)(2)(i)	A.9.1.4, A.14.1.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CP-7	Alternate Processing Site		5325 Business Continuity with Technology Recovery 5325.4 Alternate Storage and Processing Site		9.3.6.6 Alternate Processing Site	164.308(a)(7)(ii)(B), 164.310(a)(2)(i)	A.9.1.4, A.14.1.3
CP-8	Telecommunications Services		5305.8 Provisions for Agreements with State and Non-State Entities 5325.5 Telecommunications Services			164.308(a)(7)(ii)(B)	A.9.2.2, A.14.1.3
CP-9	Information System Backup		5325.6 Information System Backups	Critical Control 8: Data Recovery Capability	9.3.6.7 Information System Backup	164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.310(d)(2)(iv), 164.312(c)(1)	A.10.5.1, A.14.1.3, A.15.1.3
CP-10	Information System Recovery and Reconstitution		5325 Business Continuity with Technology Recovery 5325.1 Technology Recovery Plan	Critical Control 8: Data Recovery Capability	9.3.6.8 Information System Recovery and Reconstitution	164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C)	A.14.1.3
Identification and Authentication Family							
IA-2	Identification and Authentication (Information Asset Users)		5360 Identity and Access Management	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 13: Boundary Defense.	9.3.7.2 Identification and Authentication (Organizational Users)	164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d)	A.10.9.1, A.10.9.2, A.11.4.2, A.11.5.1, A.11.5.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
IA-3	Device Identification and Authentication		5360 Identity and Access Management		9.3.7.3 Device Identification and Authentication	164.312(a)(2)(i), 164.312(d)	A.11.4.2, A.11.4.3
IA-4	Identifier Management		5360 Identity and Access Management		9.3.7.4 Identifier Management	164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d)	A.11.2.1, A.11.5.2
IA-5	Authenticator Management		5350.1 Encryption 5360 Identity and Access Management	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	9.3.7.5 Authenticator Management Secure Storage—IRC 6103(p)(4)(B) Section 4.0	164.308(a)(5)(ii)(D)	A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.1, A.11.5.2, A.11.5.3
IA-6	Authenticator Feedback		5360 Identity and Access Management		9.3.7.6 Authenticator Feedback	164.308(a)(5)(ii)(D)	A.11.5.1, A.11.5.3
IA-7	Cryptographic Module Authentication		5350.1 Encryption 5360 Identity and Access Management	9.3.7.7 Cryptographic Module Authentication (IA-7) 7.0 Reporting Requirements—6103(p)(4)(E); (7.1.2 Encryption Requirements)		164.308(a)(5)(ii)(D)	A.15.1.6
IA-11	Re-authentication		5360 Identity and Access Management				A.11.5.6
Incident Response Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
IR-1	Incident Response Policy and Procedures		5340 Information Security Incident Management	Critical Control 18: Incident Response Capability	9.3.8.1 Incident Response Policy and Procedures 10.0 Reporting Improper Inspections or Disclosures; (10.1 General)	164.308(a)(6)(i)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.13.1.1, A.13.2.1, A.15.1.1, A.15.2.1
IR-2	Incident Response Training		5340.1 Incident Response Training	Critical Control 18: Incident Response Capability	9.3.8.2 Incident Response Training	164.308(a)(6)(i)	A.8.2.2, A.10.4.1
IR-3	Incident Response Testing		5340.2 Incident Response Testing		9.3.8.3 Incident Response Testing	164.308(a)(6)(i)	None
IR-4	Incident Handling		5340.3 Incident Handling	Critical Control 18: Incident Response Capability. Critical Control 19: Secure Network Engineering	9.3.8.4 Incident Handling 10.0 Reporting Improper Inspections or Disclosures; (10.2 Office of Safeguards Notification Process)	164.308(a)(6)(ii)	A.6.1.2, A.6.1.6, A.13.2.1, A.13.2.2, A.13.2.3
IR-5	Incident Monitoring		5340 Information Security Incident Management	Critical Control 18: Incident Response Capability	9.3.8.5 Incident Monitoring	164.308(a)(1)(ii)(D), 164.308(a)(6)(ii)	None

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
IR-6	Incident Reporting		5340.4 Incident Reporting	Critical Control 18: Incident Response Capability	9.3.8.6 Incident Reporting 10.0 Reporting Improper Inspections or Disclosures; (10.3 Incident Response Procedures) 10.0 Reporting Improper Inspections or Disclosures; (10.4 Incident Response Notification to Impacted Individuals)	164.308(a)(1)(ii)(D), 164.308(a)(6)(ii), 164.314(a)(2)(i)	A.6.1.6, A.13.1.1
IR-7	Incident Response Assistance		5340 Information Security Incident Management 5340.3 Incident Handling		9.3.8.7 Incident Response Assistance	164.308(a)(6)(ii)	A.6.1.6
IR-8	Incident Response Plan		5340 Information Security Incident Management 5340.3 Incident Handling		9.3.8.8 Incident Response Plan (IR-8) Reporting Improper Inspections or Disclosures Section 10.0 (10.3)		A.10.4.1
Maintenance Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
MA-1	System Maintenance Policy and Procedures		5315 Information Security Integration		9.3.9.1 System Maintenance Policy and Procedures	164.310(a)(2)(iv)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
MA-2	Controlled Maintenance		5315 Information Security Integration		9.3.9.2 Controlled Maintenance	164.310(a)(2)(iv)	A.9.2.4, A.9.2.7, A.11.4.4
MA-3	Maintenance Tools		5315 Information Security Integration		9.3.9.3 Maintenance Tools		A.9.2.4, A.10.4.1
MA-4	Nonlocal Maintenance		5315 Information Security Integration		9.3.9.4 Non-Local Maintenance		A.9.2.4, A.11.4.4
MA-5	Maintenance Personnel		5315 Information Security Integration		9.3.9.5 Maintenance Personnel	164.308(a)(3)(ii)(A)	A.9.1.1, A.9.2.4, A.12.4.3
MA-6	Timely Maintenance		5315 Information Security Integration			164.310(a)(2)(iv)	A.9.2.4
Media Protection Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
MP-1	Media Protection Policy and Procedures		5350.1 Encryption 5365.2 Media Protection		9.3.10.1 Media Protection Policy and Procedures Secure Storage—IRC 6103(p)(4)(B) Section 4.0	164.310(d)(1)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.7.1, A.11.1.1, A.11.3.3, A.12.3.1, A.15.1.1, A.15.1.3, A.15.2.1
MP-2	Media Access		5350.1 Encryption 5365.2 Media Protection	Critical Control 17: Data Loss Prevention	9.3.10.2 Media Access	164.308(a)(3)(ii)(A), 164.310(c, 164.310(d)(1), 164.312(c)(1)	A.7.2.2, A.10.7.3, A.11.3.3
MP-3	Media Marking		5365.2 Media Protection	Critical Control 15: Controlled Access Based on the Need to Know	9.3.10.3 Media Marking 5.0 Restricting Access—IRC 6103(p)(4)©; (5.1)	164.310(c , 164.310(d)(1)	A.7.2.2, A.10.7.3, A.10.7.4
MP-4	Media Storage		5350.1 Encryption 5365.2 Media Protection	Critical Control 17: Data Loss Prevention	9.3.10.4 Media Storage 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.6 Media Off-Site Storage Requirements)	164.310(c, 164.310(d)(1), 164.310(d)(2)(iv)	A.10.7.1, A.10.7.4, A.11.3.3, A.15.1.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
MP-5	Media Transport		5350.1 Encryption 5365.2 Media Protection		9.3.10.5 Media Transport 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.6 Media Off-Site Storage Requirements)	164.310(d)(1), 164.310(d)(2)(iii), 164.312(c)(1)	A.9.2.5, A.9.2.7, A.10.7.1, A.10.8.3
MP-6	Media Sanitization		5365.3 Media Disposal		9.3.10.6 Media Sanitization (MP-6) 3.0 Record Keeping Requirement (3.3 Converted Media) 8.0 Disposing of FTI—IRC 6103(p)(4)(F); (8.3 Destruction and Disposal)	164.310(d)(1), 164.310(d)(2)(i), 164.310(d)(2)(ii)	A.9.2.6, A.10.7.1, A.10.7.2
MP-7	Media Use		5365.2 Media Protection				A.10.4.1, A.10.7.1
Physical and Environmental Protection Family							
PE-2	Physical Access Authorizations		5335 Information Security Monitoring 5365 Physical Security		9.3.11.2 Physical Access Authorizations Secure Storage—IRC 6103(p)(4)(B) Section 4.0	164.310(a)(1), 164.310(a)(2)(iii)	A.8.3.3, A.9.1.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PE-3	Physical Access Control		5365 Physical Security		9.3.11.3 Physical Access Control (PE-3) Secure Storage—IRC 6103(p)(4)(B) Section 4.0; (4.3) 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.5 Physical Security of Computers, Electronic, and Removable Media)	164.310(a)(1), 164.310(a)(2)(iii), 164.310(b), 164.310(c	A.9.1.1, A.9.1.2, A.9.1.3, A.9.1.6, A.11.4.4
PE-4	Access Control for Transmission Medium		5365 Physical Security		9.3.11.4 Access Control for Transmission Medium	164.310(a)(1), 164.310(c	A.9.1.1, A.9.1.2, A.9.1.3, A.9.2.3
PE-5	Access Control for Output Devices		5365 Physical Security 5365.1 Access Control for Output Devices		9.3.11.5 Access Control for Output Devices	164.310(a)(1), 164.310(b), 164.310(c	A.9.1.1, A.9.1.2, A.9.1.3
PE-6	Monitoring Physical Access		5335 Information Security Monitoring 5335.1 Continuous Monitoring 5335.2 Auditable Events 5365 Physical Security		9.3.11.6 Monitoring Physical Access Secure Storage—IRC 6103(p)(4)(B) Section 4.0 (4.5)	164.310(a)(2)(iii)	A.9.1.2, A.10.10.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PE-8	Visitor Access Records		5335 Information Security Monitoring 5335.1 Continuous Monitoring 5335.2 Auditable Events 5365 Physical Security		9.3.11.7 Visitor Access Records	164.310(a)(2)(iii)	A.9.1.2, A.10.10.2
PE-9	Power Equipment and Cabling		5300.5 Minimum Security Controls 5365 Physical Security		Secure Storage—IRC 6103(p)(4)(B); (4.7.1 Equipment)		A.9.1.4, A.9.2.2, A.9.2.3
PE-10	Emergency Shutoff		5300.5 Minimum Security Controls 5365 Physical Security				A.9.2.2
PE-11	Emergency Power		5300.5 Minimum Security Controls 5365 Physical Security				A.9.2.2
PE-12	Emergency Lighting		5300.5 Minimum Security Controls 5365 Physical Security				A.9.2.2
PE-13	Fire Protection		5300.5 Minimum Security Controls 5365 Physical Security				A.6.1.6, A.9.1.4, A.9.2.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PE-14	Temperature and Humidity Controls		5300.5 Minimum Security Controls 5335.1 Continuous Monitoring 5365 Physical Security				A.9.2.1, A.9.2.2
PE-15	Water Damage Protection		5300.5 Minimum Security Controls 5335.1 Continuous Monitoring 5365 Physical Security				A.9.1.4, A.9.2.1
PE-16	Delivery and Removal		5365 Physical Security		9.3.11.8 Delivery and Removal		A.9.1.6, A.9.2.7
PE-17	Alternate Work Site		5365 Physical Security		9.3.11.9 Alternate Work Site	164.310(a)(2)(i)	A.9.2.5, A.11.7.2
PE-19	Information Leakage		5365 Physical Security				A.9.1.4, A.9.2.1, A.12.5.4
Planning Family							
PL-4	Rules of Behavior		5305.8 Provisions for Agreements with State and Non-State Entities		9.3.12.3 Rules of Behavior		A.6.1.5, A.6.2.2, A.6.2.3, A.7.1.3. A.8.1.1, A.8.1.3, A.8.2.1, A.10.8.1, A.11.7.1, A.11.7.2, A.13.1.2, A.15.1.5

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PL-8	Information Security Architecture		5315 Information Security Integration				A.12.1.1
Personnel Security							
PS-4	Personnel Termination		5305.4 Personnel Management		9.3.13.4 Termination	164.308(a)(3)(ii)(C)	A.8.3.1, A.8.3.2, A.8.3.3
PS-5	Personnel Transfer		5305.4 Personnel Management		9.3.13.5 Personnel Transfer	164.308(a)(3)(ii)(C)	A.8.3.1, A.8.3.2, A.8.3.3
PS-6	Access Agreements		5305.4 Personnel Management 5315 Information Security Integration		9.3.13.6 Access Agreements (PS-6) 11.0 Disclosure to Other Persons; (11.2 Authorized Disclosures Precautions) 11.0 Disclosure to Other Persons; (11.3 Disclosing FTI to Contractors)	164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(B), 164.310(b), 164.310(d)(2)(iii), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	A.6.1.5, A.6.2.3, A.7.1.3, A.8.1.1, A.8.1.3, A.8.2.1, A.10.8.1, A.11.7.1, A.11.7.2, A.15.1.5
Risk Assessment Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
RA-5	Vulnerability Scanning		5330.1 Security Assessments 5335 Information Security Monitoring 5335.1 Continuous Monitoring 5345 Vulnerability and Threat Management	Critical Control 4: Continuous Vulnerability Assessment and Remediation. Critical Control 6: Application Software Security. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 13: Boundary Defense. Critical Control 20: Penetration Tests and Red Team Exercises.	9.3.14.3 Vulnerability Scanning		A.12.6.1, A.15.2.2
System and Services Acquisition Family							
SA-3	System Development Life Cycle		5315 Information Security Integration 5315.2 System Development Lifecycle	Critical Control 6: Application Software Security	9.3.15.3 System Development Life Cycle		A.6.1.3, A.12.1.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SA-4	Acquisition Process		5305.8 Provisions for Agreements with State and Non-State Entities 5315 Information Security Integration 5315.1 System and Services Acquisition	Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 6: Application Software Security.	9.3.15.4 Acquisition Process	164.314(a)(2)(i)	A.10.3.2, A.12.1.1, A.12.5.5
SA-5	Information System Documentation		5315 Information Security Integration 5315.3 Information Asset Documentation		9.3.15.5 Information System Documentation		A.10.1.1, A.10.7.4, A.13.1.2, A.15.1.3
SA-8	Security Engineering Principles		5315 Information Security Integration	Critical Control 6: Application Software Security. Critical Control 19: Secure Network Engineering.	9.3.15.6 Security Engineering Principles		A.10.4.2, A.12.1.1
SA-9	External Information System Services		5305.8 Provisions for Agreements with State and Non-State Entities 5315.1 System and Services Acquisition		9.3.15.7 External Information System Services	164.308(b)(1), 164.308(b)(4), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	A.6.1.3, A.6.1.5, A.6.2.1, A.6.2.2, A.6.2.3, A.8.2.1, A.10.2.1, A.10.2.2, A.10.2.3, A.10.6.2, A.10.8.2, A.12.5.5

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SA-10	Developer Configuration Management		5315.1 System and Services Acquisition 5315.5 Configuration Management		9.3.15.8 Developer Configuration Management		A.10.1.2, A.10.1.4, A.10.2.3, A.10.3.2, A.12.4.3, A.12.5.1, A.12.5.3, A.12.5.5
SA-11	Developer Security Testing and Evaluation		5315.1 System and Services Acquisition 5315.4 System Developer Security Testing		9.3.15.9 Developer Security Testing and Evaluation		A.6.1.8, A.10.3.2, A.12.5.5, A.13.1.2
System and Communications Protection Family							
SC-2	Application Partitioning		5350 Operational Security		9.3.16.2 Application Partitioning		A.10.4.2, A.10.9.2, A.11.4.5, A.11.5.4
SC-4	Information In Shared Resources		5350 Operational Security		9.3.16.3 Information in Shared Resources		None
SC-5	Denial of Service Protection		5350 Operational Security		9.3.16.4 Denial of Service Protection		A.10.3.1, A.10.6.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SC-7	Boundary Protection		5350 Operational Security	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services. Critical Control 13: Boundary Defense.	9.3.16.5 Boundary Protection		A.10.4.1, A.10.4.2, A.10.6.1, A.10.8.1, A.10.8.4, A.10.9.1, A.10.9.2, A.10.10.2, A.11.4.1, A.11.4.5, A.11.4.6, A.11.4.7, A.11.6.2
SC-8	Transmission Confidentiality and Integrity		5350 Operational Security 5350.1 Encryption		9.3.16.6 TRANSMISSION CONFIDENTIALITY AND INTEGRITY 4.0 SECURE STORAGE—IRC 6103(P)(4)(B); (4.4 FTI IN TRANSIT) 7.0 REPORTING REQUIREMENTS—6103(P)(4)(E); (7.1.2 ENCRYPTION REQUIREMENTS)	164.312(C)(1), 164.312(C)(2), 164.312(E)(2)(I)	A.10.6.1, A.10.8.1, A.10.8.4, A.10.9.1, A.10.9.2, A.12.2.3
SC-10	Network Disconnect		5350 Operational Security		9.3.16.7 Network Disconnect		A.10.6.1, A.11.3.2, A.11.5.5

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SC-12	Cryptographic Key Establishment and Management		5350 Operational Security 5350.1 Encryption		9.3.16.8 Cryptographic Key Establishment and Management 7.0 Reporting Requirements—6103(p)(4)(E); (7.1.2 Encryption Requirements)	164.312(e)(2)(ii)	A.12.3.2
SC-13	Cryptographic Protection		5350 Operational Security 5350.1 Encryption	Critical Control 17: Data Loss Prevention	9.3.16.9 Cryptographic Protection 7.0 Reporting Requirements—6103(p)(4)(E); (7.1.2 Encryption Requirements)	164.312(a)(2)(iv), 164.312(e)(2)(ii)	A.10.9.1, A.10.9.2, A.15.1.6
SC-15	Collaborative Computing Devices		5350 Operational Security		9.3.16.10 Collaborative Computing Devices		A.10.8.1
SC-17	Public Key Infrastructure Certificates		5350 Operational Security 5350.1 Encryption		9.3.16.11 Public Key Infrastructure Certificates		A.12.3.2
SC-18	Mobile Code		5350 Operational Security	Critical Control 5: Malware Defenses. Critical Control 13: Boundary Defense	9.3.16.12 Mobile Code		A.10.4.2, A.12.4.1
SC-19	Voice Over Internet Protocol		5350 Operational Security		9.3.16.13 Voice over Internet Protocol 9.4.15 VoIP Systems		None

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SC-20	Secure Name/Address Resolution Service (Authoritative Source)		5350 Operational Security	Critical Control 19: Secure Network Engineering			A.10.6.1
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)		5350 Operational Security	Critical Control 19: Secure Network Engineering			A.10.6.1
SC-22	Architecture and Provisioning for Name/Address Resolution Service		5350 Operational Security	Critical Control 19: Secure Network Engineering			A.10.6.1
SC-23	Session Authenticity		5350 Operational Security 5350.1 Encryption		9.3.16.14 Session Authenticity		None
SC-28	Protection of Information at Rest		5350 Operational Security 5350.1 Encryption	Critical Control 17: Data Loss Prevention	9.3.16.15 Protection of Information at Rest		None
SC-39	Process Isolation		5350 Operational Security		9.4.1 Cloud Computing Environments 9.4.11 Storage Area Networks 9.4.14 Virtualization Environments		None
SC-40	Wireless Link Protection		5350 Operational Security		9.4.18 Wireless Networks		None
System and Information Integrity Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SI-1	System and Information Integrity Policy and Procedures		5350 Operational Security		9.3.17.1 System and Information Integrity Policy and Procedures	164.312(c)(1)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.4.1, A.15.1.1, A.15.2.1
SI-2	Flaw Remediation		5350 Operational Security		9.3.17.2 Flaw Remediation		A.12.6.1, A.13.1.2
SI-3	Malicious Code Protection		5350 Operational Security 5355 Endpoint Defense 5355.1 Malicious Code Protection	Critical Control 5: Malware Defenses Critical Control 6: Application Software Security	9.3.17.3 Malicious Code Protection	164.308(a)(5)(ii)(B)	A.10.4.1, A.10.9.3
SI-4	Information System Monitoring		5335.1 Continuous Monitoring 5350 Operational Security	Critical Control 7: Wireless Device Control. Critical Control 13: Boundary Defense. Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs. Critical Control 17: Data Loss Prevention.	9.3.17.4 Information System Monitoring	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	A.10.9.3, A.10.10.2, A.10.10.3, A.15.3.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SI-7	Software, Firmware, and Information Integrity		5300.5 Minimum Security Controls 5350 Operational Security	Critical Control 3: Secure Configurations for Hardware and Software		164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)	A.10.4.1, A.10.9.3, A.10.10.2, A.12.2.2, A.12.2.3, A.12.4.1
SI-8	Spam Protection		5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.6 Spam Protection	164.308(a)(5)(ii)(B)	None
SI-10	Information Input Validation		5300.5 Minimum Security Controls 5350 Operational Security	Critical Control 6: Application Software Security	9.3.17.7 Information Input Validation		A.10.7.3, A.10.9.3, A.12.2.1, A.12.2.2
SI-11	Error Handling		5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.8 Error Handling		None
SI-12	Information Handling and Retention		5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.9 Information Handling and Retention		A.10.7.3, A.15.1.3, A.15.1.4
SI-16	Memory Protection		5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.10 Memory Protection		None

System Security Plan Privacy Control		SCO Information Security Program Standard(s)	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	Information Practices Act of 1977 (State) *(California Civil Code, Title 1.8 Personal Data, Chapter 1 [§1798-1798.78])*	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	The Privacy Act of 1974 (Federal)
AP-1	Authority and Purpose	500 Privacy Standards	5310 Privacy	1798.14, 1798.24, 1798.30			5 U.S.C. § 552a (e)
AP-2	Purpose Specification	500 Privacy Standards	5310 Privacy	1798.17, 1798.24, 1798.30, 1798.60			5 U.S.C. § 552a (e)(3)(A)-(B)
AR-3	Privacy Requirements for Contractors and Service Providers	500 Privacy Standards	5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.19, 1798.20, 1798.21, 1798.24		164.308(b)(1), 164.308(b)(4), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	5 U.S.C. § 552a(m)
AR-4	Privacy Monitoring and Auditing	122 Risk Assessment 130 Security Compliance 203 Project System Security Plans 101 User Activity Monitoring Notice 406 Audit Trails	5310 Privacy 5310.3 Limiting Use and Disclosure	1798.22	Other Safeguards—IRC 6103(p)(4)(D) Section 6.0	164.312(b), 164.308(a)(1)(ii)(D)	5 U.S.C. § 552a

System Security Plan Privacy Control		SCO Information Security Program Standard(s)	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	Information Practices Act of 1977 (State) *(California Civil Code, Title 1.8 Personal Data, Chapter 1 [§1798-1798.78])*	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	The Privacy Act of 1974 (Federal)
AR-7	Privacy-Enhanced System Design and Development	122 Risk Assessment 130 Security Compliance 203 Project System Security Plans	5305.8 Provisions for Agreements with State and Non-State Entities 5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.20, 1798.21			5 U.S.C. § 552a(e)(10)
AR-8	Accounting for Disclosures	101-User Access Monitoring Notice 406 Audit Trails 500 Privacy Standards	5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.25, 1798.27		164.312(b), 164.308(a)(1)(ii)(D)	5 U.S.C. § 552a (c)(1), (c)(3), (j), (k)
DI-1	Data Quality	500 Privacy Standards	5310 Privacy 5310.5 Information Integrity 5310.7 Security Safeguards	1798.15, 1798.16, 1798.18		164.312(e)(2)(i), 164.312(c)(2)	5 U.S.C. § 552a (c) and (e)
DM-1	Minimization of Personally Identifiable Information	122 Risk Assessment 130 Security Compliance 500 Privacy Standards	5310 Privacy 5310.2 Limiting Collection	1798.24			5 U.S.C. §552a (e)

System Security Plan Privacy Control		SCO Information Security Program Standard(s)	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	Information Practices Act of 1977 (State) *(California Civil Code, Title 1.8 Personal Data, Chapter 1 [§1798-1798.78])*	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	The Privacy Act of 1974 (Federal)
DM-2	Data Retention and Disposal	122 Risk Assessment 130 Security Compliance 500 Privacy Standards	5310 Privacy 5310.5 Information Integrity 5310.6 Data Retention and Destruction 5310.7 Security Safeguards	1798.18, 1798.27, 1798.64			5 U.S.C. § 552a (e)(1), (c)(2)
DM-3	Minimization of PII Used in Testing, Training, and Research	122 Risk Assessment 130 Security Compliance 500 Privacy Standards	5310 Privacy 5310.7 Security Safeguards	1798.21			
SE-1	Inventory of Personally Identifiable Information	207 System Inventory	5305.5 Information Asset Management 5310 Privacy 5310.6 Data Retention and Destruction 5310.7 Security Safeguards	1798.18, 1798.21		164.310(d)(1), 164.310(d)(2)(iii)	5 U.S.C. § 552a (e) (10)

System Security Plan Privacy Control		SCO Information Security Program Standard(s)	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	Information Practices Act of 1977 (State) *(California Civil Code, Title 1.8 Personal Data, Chapter 1 [§1798-1798.78])*	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	The Privacy Act of 1974 (Federal)
SE-2	Privacy Incident Response	122 Risk Assessment 130 Security Compliance 203 Project System Security Plans 317 Information Security Incident Reporting SCO Information Memorandum 07-07	5310 Privacy 5310.7 Security Safeguards	1798.21, 1798.29		164.308(a)(6)(i), 164.308(a)(6)(ii)	5 U.S.C. § 552a (e), (i)(1), and (m)
TR-1	Privacy Notice	500 Privacy Standards	5310 Privacy 5310.1 State Entity Privacy Statement and Notice on Collection 5310.5 Information Integrity SIMM 5310-A	1798.17, 1798.32 California Government Code § 11019.9			5 U.S.C. § 552a (e)(3), (e)(4)

System Security Plan Privacy Control		SCO Information Security Program Standard(s)	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	Information Practices Act of 1977 (State) *(California Civil Code, Title 1.8 Personal Data, Chapter 1 [§1798-1798.78])*	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	The Privacy Act of 1974 (Federal)
UL-1	Internal Use	122 Risk Assessment 203 Project System Security Plans 500 Privacy Standards	5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.17, 1798.24		164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(1)(ii)(D)	5 U.S.C. § 552a (b)(1)
UL-2	Information Sharing with Third Parties	500 Privacy Standards	5305.8 Provisions for Agreements with State and Non-State Entities 5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.17, 1798.20, 1798.21, 1798.24		164.308(b)(1), 164.308(b)(4), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o)

MEKETA

Merced County Employees' Retirement Association

February 22, 2024

Asset Allocation Review and Risk Analysis

Background

→ Meketa Investment Group updates our Capital markets expectations (CMEs) annually. Meketa presents the current MercedCERA policy target Asset Allocation (in effect as of November, 2021) with the 2024 CMEs as part of our continued review process in determining the long-term risk and return expectations for the MercedCERA portfolio.

→ In addition to the current policy targets, Meketa has prepared 3 alternate allocation proposals with varying degrees of risk/return. Option A and Option B reflect the risk averse sentiment of the trustee risk survey results, whereas Option C presents an alternate allocation that reflects similar risk/return profiles as the current policy target.

→ As mentioned above, these options were in part driven by the trustee risk survey results and are not meant to be adopted as changes to the current allocation. Instead, the intention is for the different options to drive discussions on what asset allocation changes the Board would like to see implemented. In April, Meketa plans to bring refined asset allocation options for Board consideration

→ The analytics presented are consistent with what has been presented in previous meetings – we review the expected return, standard deviation, and historical and prospective risk scenarios.

→ Note that expected returns for most asset classes decreased in 2024. This is due partially to the strong rallies in 2023 resulting in higher valuations at year end.

What is driving the changes from last year?

→ Credit spreads tightened, leading to lower yields, thus decreasing expected returns for fixed income assets.

→ Most equity markets rallied, pushing them to higher valuations, thus reducing their forward-looking returns.

→ Lower anticipated borrowing costs had a positive impact on assets that use leverage.

→ Lower anticipated cash yields hurt expected returns for hedge funds and related asset classes.

→ The long downward trend in cap rates for real estate reversed, pushing up their expected returns.

→ Higher anticipated long-term interest rates also provide a tailwind in our 20-year projections, as the bridge from 10 to 20 years is made via a risk premium being added to a (higher) future risk-free rate.

- The risk-free rate jumped from 4.17% to 4.64%.

→ The changes we made to several models also had an impact:

- We reweighted our private market composites to reflect a blend of the market opportunity and a typical client portfolio.
- We reduced the cap for the magnitude of currency impact from +/- 100 bp to +/- 50 bp per annum.
- We increased the % of GDP growth that translates to EPS growth for the US, while decreasing it for most other equity markets.
- We extended our look-back period from 15 years to 20 years for historical volatility (and correlations).

20-Year Risk-Return Expectations

→ In comparison to the expected outcomes according to the 2023 Capital Market Expectations (CME) :

- Long-term (20-year) expected return decreased,
- Risk, as measured by standard deviation, also decreased, and Sharpe Ratio increased.

Merced County Employees' Retirement Association

	2024 CME	2023 CME	Change
Expected Return	8.5%	8.8%	-0.3%
Standard Deviation	13.2%	13.8%	-0.6%
Sharpe Ratio	0.46	0.43	0.03

20-Year Return Expected by Asset Class

Asset Class	2023 20Y Expected Return	2024 20Y Expected Return	Change in Expected Return	MCERA Current Policy Allocations (%)
Public Equity	--	--	--	**41.0**
US Equity	8.7	8.5	-0.2	22.0
Developed Market Equity (non-US)	9.8	8.9	-0.9	11.0
Emerging Market Equity	10.0	8.9	-1.1	8.0
Private Equity	11.0	11.2	+0.2	**15.0**
Public Fixed Income	--	--	--	**16.0**
Investment Grade Bonds	4.7	4.8	+0.1	11.0
Bank Loans[1]	7.0	6.6	-0.4	2.5
High Yield[1]	7.3	6.8	-0.5	2.5
Direct Lending	8.3	8.4	+0.1	**5**
Private Markets	--	--	--	**13.0**
Core Private Real Estate	6.5	6.9	+0.4	8.0
Natural Resources (Private)	9.8	9.3	-0.5	2.5
Infrastructure (Core Private)	7.8	8.0	+0.2	2.5
Hedge Funds	6.1	5.8	-0.3	**10.0**
Cash Equivalents	2.9	2.5	-0.4	**0.0**

[1] Opportunistic Credit is modeled as 50/50 Bank Loans and High Yield

Correlation Data

	Inv. Grade Bonds	Long-term Gov't Bonds	TIPS	High Yield Bonds	US Equity	Dev. Non-US Equity	Em. Market Equity	Private Equity	Real Estate	Commod.	Infra.	Hedge Funds
Investment Grade Bonds	1.00											
Long-term Government Bonds	0.86	1.00										
TIPS	0.77	0.61	1.00									
High Yield Bonds	0.35	-0.04	0.46	1.00								
US Equity	0.22	-0.10	0.30	0.76	1.00							
Developed Non-US Equity	0.26	-0.09	0.33	0.76	0.88	1.00						
Emerging Market Equity	0.27	-0.05	0.36	0.72	0.74	0.86	1.00					
Private Equity	0.00	-0.10	0.03	0.66	0.90	0.83	0.79	1.00				
Real Estate	0.26	0.06	0.17	0.56	0.53	0.49	0.43	0.49	1.00			
Commodities	0.00	-0.23	0.28	0.47	0.46	0.55	0.58	0.23	0.15	1.00		
Infrastructure	0.31	0.14	0.32	0.65	0.64	0.68	0.60	0.51	0.61	0.41	1.00	
Hedge Funds	0.12	-0.20	0.30	0.78	0.80	0.83	0.81	0.53	0.47	0.64	0.61	1.00

Proposed Policy Options

Asset Allocation Policy Options[1]

	Current Policy Targets (%)	Option A: Lower Risk (%)	Option B: Even Lower Risk, higher FI (%)	Option C: Same risk, different composition (%)
Public Equity	41	34	25	44
US Equity	22	22	16	26
Developed Market Equity (non-US)	11	9	6.5	13
Emerging Market Equity	8	4	2.5	5
Private Equity	15	15	12	13
Public Fixed Income	16	22	37	18
US Fixed Income	11	17	30	14
Opportunistic Credit	6	6	8	4
Direct Lending	5	5	5	5
Core Private Real Estate	8	8	8	8
Natural Resources (Private)	2.5	2.5	2.5	2.5
Infrastructure (Core Private)	2.5	2.5	2.5	2.5
Hedge Funds	10	10	5	7
Cash Equivalents	0	1	3	0
Expected Return (20 years)	8.5	8.2	7.6	8.4
Standard Deviation	13.2	11.9	9.8	12.9
Probability of Achieving 7% over 20 Years	69.7	67.5	61.2	69.0

[1] Expected return and standard deviation are based upon Meketa Investment Group's Annual Capital Markets Expectations (CMEs). Throughout this document, returns for periods longer than one year are annualized.

Public Fixed Income represents the asset class Investment Grade Bonds in Meketa's CMEs. Opportunistic Fixed Income represents an equal blend of Bank Loans and High Yield asset classes in Meketa's CMEs

MPT-Based Risk Analysis

Scenario	Current Policy Targets (%)	Option A: Lower Risk (%)	Option B: Even Lower Risk, higher FI (%)	Option C: Same risk, different composition (%)
Worst Case Returns (1)				
OneYear (annualized)	-17.9	-16.1	-12.8	-17.6
ThreeYears (annualized)	-7.7	-6.6	-4.7	-7.4
FiveYears (annualized)	-4.2	-3.4	-2.0	-4.1
TenYears (annualized)	-0.7	-0.2	0.7	-0.6
TwentyYears (annualized)	1.9	2.2	2.7	2.0
Probability of Experiencing Negative Returns				
OneYear	24.9	23.6	20.8	24.7
ThreeYears	12.0	10.6	8.0	11.8
FiveYears	6.5	5.4	3.5	6.3
TenYears	1.6	1.1	0.5	1.5
TwentyYears	0.1	0.1	0.0	0.1
Probability of Achieving at least a 7% Return				
OneYear	54.6	54.0	52.5	54.4
ThreeYears	57.9	57.0	54.4	57.6
FiveYears	60.2	59.0	55.7	59.8
TenYears	64.2	62.6	58.0	63.7
TwentyYears	69.7	67.5	61.2	69.0

Historical Negative Scenario Analysis[1] (*Cumulative* Return)

Scenario	Current Policy Targets (%)	Option A: Lower Risk (%)	Option B: Even Lower Risk, higher FI (%)	Option C: Same risk, different composition (%)
Post-COVID Rate Hikes(Jan 2022-Oct 2023)	-6.0	-5.6	-6.3	-6.5
COVID-19 Market Shock (Feb 2020-Mar 2020)	-17.6	-15.4	-12.2	-18.1
Taper Tantrum (May - Aug 2013)	0.7	0.9	0.2	0.8
Global Financial Crisis (Oct 2007 - Mar 2009)	-27.4	-23.3	-16.5	-27.2
Popping of the TMT Bubble (Apr 2000 - Sep 2002)	-16.9	-11.9	-3.1	-16.8
LTCM (Jul - Aug 1998)	-8.3	-6.6	-4.4	-7.9
Asian Financial Crisis (Aug 97 - Jan 98)	2.3	4.2	4.7	3.1
Rate spike (1994 Calendar Year)	3.8	3.8	2.8	3.7
Early 1990s Recession (Jun - Oct 1990)	-5.4	-4.2	-2.6	-5.5
Crash of 1987 (Sep - Nov 1987)	-10.9	-9.1	-6.2	-11.2
Strong dollar (Jan 1981 - Sep 1982)	1.2	4.2	9.6	2.2
Volcker Recession (Jan - Mar 1980)	-3.6	-3.6	-4.1	-3.8
Stagflation (Jan 1973 - Sep 1974)	-21.7	-18.2	-12.0	-21.6

→ Options A & B have considerable less weight to equities and as a result fare better in historical equity market downturns

[1] See the Appendix for our scenario inputs. In periods where the ideal benchmark was not yet available we used the next closest benchmark(s) as a proxy.

Historical Positive Scenario Analysis[1] (*Cumulative* Return)

Scenario	Current Policy Targets (%)	Option A: Lower Risk (%)	Option B: Even Lower Risk, higher FI (%)	Option C: Same risk, different composition (%)
Covid Recovery (Apr 2020-Dec 2021)	56.3	52.6	41.5	56.2
Global Financial Crisis Recovery (Mar 2009 - Nov 2009)	33.6	28.4	23.6	33.0
Best of Great Moderation (Apr 2003 - Feb 2004)	30.4	25.8	20.7	29.5
Peak of the TMT Bubble (Oct 1998 - Mar 2000)	48.1	42.4	32.4	44.7
Plummeting Dollar (Jan 1986 - Aug 1987)	50.9	43.1	35.0	51.4
Volcker Recovery (Aug 1982 - Apr 1983)	29.2	27.6	25.8	30.5
Bretton Wood Recovery (Oct 1974 - Jun 1975)	27.4	24.6	20.4	28.0

→ The Current Policy and Option C, given their higher equity allocations, capture more of the equity market recovery than Options A & B.

[1] See the Appendix for our scenario inputs. In periods where the ideal benchmark was not yet available we used the next closest benchmark(s) as a proxy.

Stress Testing: Impact of Market Movements (Expected Return under Stressed Conditions)[1]

Scenario	Current Policy Targets (%)	Option A: Lower Risk (%)	Option B: Even Lower Risk, higher FI (%)	Option C: Same risk, different composition (%)
10-year Treasury Bond rates rise 100 bps	4.5	3.6	2.1	4.3
10-year Treasury Bond rates rise 200 bps	-1.1	-1.7	-2.6	-1.4
10-year Treasury Bond rates rise 300 bps	-2.9	-3.5	-4.6	-3.0
Baa Spreads widen by 50 bps, High Yield by 200 bps	0.1	0.4	1.0	0.2
Baa Spreads widen by 300 bps, High Yield by 1000 bps	-21.7	-19.0	-15.0	-21.3
Trade Weighted Dollar gains 10%	-4.2	-3.1	-2.2	-3.9
Trade Weighted Dollar gains 20%	-1.8	-0.8	0.3	-1.2
U.S. Equities decline 10%	-6.1	-5.3	-3.8	-5.9
U.S. Equities decline 25%	-17.0	-15.1	-11.8	-16.7
U.S. Equities decline 40%	-25.2	-22.4	-17.7	-25.2

[1] Assumes that assets not directly exposed to the factor are affected nonetheless. See the Appendix for further details.

Stress Testing: Impact of Positive Market Movements (Expected Return under Positive Conditions)[1]

Scenario	Current Policy Targets (%)	Option A: Lower Risk (%)	Option B: Even Lower Risk, higher FI (%)	Option C: Same risk, different composition (%)
10-year Treasury Bond rates drop 100 bps	1.9	2.1	2.3	1.9
10-year Treasury Bond rates drop 200 bps	9.2	8.6	8.1	9.6
10-year Treasury Bond rates drop 300 bps	11.4	10.8	10.7	12.0
Baa Spreads narrow by 30bps, High Yield by 100 bps	7.5	7.0	5.7	7.5
Baa Spreads narrow by 100bps, High Yield by 300 bps	13.4	11.7	10.0	12.9
Trade Weighted Dollar drops 10%	7.6	6.6	5.6	7.3
Trade Weighted Dollar drops 20%	20.2	17.7	15.1	20.4
U.S. Equities rise 10%	6.6	6.2	5.1	6.5
U.S. Equities rise 30%	15.4	14.0	11.4	15.6

[1] Assumes that assets not directly exposed to the factor are affected nonetheless. See the Appendix for further details.

Stress Testing: Negative Inflation Scenarios (Expected Return under Stressed Conditions)[1]

Scenario	Current Policy Targets (%)	Option A: Lower Risk (%)	Option B: Even Lower Risk, higher FI (%)	Option C: Same risk, different composition (%)
Inflation slightly higher than expected	-0.2	-0.2	-0.3	-0.3
Inflation meaningfully higher than expected	-4.0	-3.7	-3.3	-4.5
Low Growth and Low Inflation	-6.7	-5.7	-4.8	-6.7
Low Growth and High Inflation	-9.6	-8.1	-6.7	-9.5
Brief, moderate inflation spike	-3.2	-2.7	-2.3	-2.9
Extended, moderate inflation spike	-6.2	-5.4	-4.3	-6.0
Brief, extreme inflation spike	-8.2	-7.1	-5.6	-7.9
Extended, extreme inflation spike	-10.9	-9.5	-7.3	-10.7

[1] Assumes that assets not directly exposed to the factor are affected nonetheless. See the Appendix for further details.

Stress Testing: Positive Inflation Scenarios (Expected Return under Stressed Conditions)[1]

Scenario	Current Policy Targets (%)	Option A: Lower Risk (%)	Option B: Even Lower Risk, higher FI (%)	Option C: Same risk, different composition (%)
High Growth and Low Inflation	11.3	9.6	7.4	11.0
High Growth and Moderate Inflation	9.6	8.2	6.3	9.3
High Growth and High Inflation	7.4	6.5	4.9	7.1

[1] Assumes that assets not directly exposed to the factor are affected nonetheless. See the Appendix for further details.

Appendices

Scenario Return Inputs

Asset Class	Benchmark Used
Investment Grade Bonds	Bloomberg US Aggregate
TIPS	Bloomberg Global Inflation Linked: US TIPS
Intermediate-term Government Bonds	Bloomberg US Treasury: Intermediate
Long-term Government Bonds	Bloomberg US Treasury: Long
EM Bonds (Local)	Bloomberg Emerging Markets Hard Currency Aggregate
Bank Loans	Credit Suisse Leveraged Loan
High Yield Bonds	Bloomberg US Corporate High Yield
Direct Lending	Cliffwater Direct Lending Index
Special Situations	Cambridge Associates Proxy IRR Returns
Real Estate	NCREIF Property Index
Core Private Real Estate	Cambridge Associates Proxy IRR Returns
Value-Added Real Estate	Cambridge Associates Proxy IRR Returns
Opportunistic Real Estate	Cambridge Associates Proxy IRR Returns
REITs	FTSE NAREIT All Equity REITS
Infrastructure (Private)	Cambridge Associates Proxy IRR Returns
Natural Resources (Private)	Cambridge Associates Proxy IRR Returns
Timber	NCREIF Timberland
Commodities	Bloomberg Commodity Index
US Equity	Russell 3000
Public Foreign Equity (Developed)	MSCI EAFE
Public Foreign Equity (Emerging)	MSCI Emerging Markets
Private Equity	Cambridge Associates Proxy IRR Returns
Long-short Equity	HFRI Equity Hedge
Global Macro	HFRI Macro
Hedge Funds	HFRI Fund Weighted Composite
Private Debt	Cambridge Associates Proxy IRR Returns

Negative Historical Scenario Returns - Sample Inputs

	Covid-19 Market Shock (Feb 2020-Mar 2020)	Taper Tantrum (May - Aug 2013)	Global Financial Crisis (Oct 2007 - Mar 2009)	Popping of the TMT Bubble (Apr 2000 - Sep 2002)	LTCM (Jul - Aug 1998)
Cash Equivalents	0.4	0.0	2.6	9.9	0.8
Short-term Investment Grade Bonds	0.4	-0.1	7.9	21.9	1.6
Investment Grade Bonds	-0.9	-3.7	8.5	28.6	1.8
Long-term Corporate Bonds	-18.4	-9.3	-10.3	26.9	-0.6
Long-term Government Bonds	12.7	-11.6	24.2	35.5	4.1
TIPS	-0.4	-8.5	8.2	37.4	0.7
Global ILBs	-6.5	-7.4	-3.9	39.7	0.7
High Yield Bonds	-20.8	-2.0	-22.8	-6.3	-5.0
Bank Loans	-20.3	0.8	-23.7	6.3	0.7
Direct Lending	-4.8	2.6	-3.3	-2.0	-2.6
Foreign Bonds	-4.5	-3.2	2.1	8.5	3.5
Asset Based Lending	-4.8	2.6	-3.3	-2.0	-2.6
Special Situations	-12.2	4.6	-26.4	-2.0	-2.6
Emerging Market Bonds (major)	-15.3	-11.5	-5.0	6.3	-28.2
Emerging Market Bonds (local)	-13.9	-14.3	-7.9	7.2	-34.1
US Equity	-35.0	3.0	-45.8	-43.8	-15.4
Developed Market Equity (non-US)	-32.7	-2.2	-52.1	-46.7	-11.5
Emerging Market Equity	-31.2	-9.4	-51.2	-43.9	-26.7
Global Equity	-33.6	-0.7	-49.3	-46.7	-14.0
Private Equity/Debt	-7.8	5.7	-27.7	-23.6	-3.2
Private Equity	-7.4	5.8	-28.2	-26.2	-3.3
Private Debt Composite	-10.1	4.6	-22.3	-1.8	-2.3
REITs	-41.0	-13.3	-63.0	45.4	-15.3
Core Private Real Estate	0.7	3.6	-10.6	23.6	2.3
Value-Added Real Estate	-3.5	3.0	-32.2	25.4	0.0
Opportunistic Real Estate	-8.6	4.0	-25.7	21.4	1.5
Natural Resources (Private)	-22.1	2.5	-31.2	-3.9	-16.9
Timberland	0.1	1.3	20.7	-1.5	0.5
Farmland	-0.1	3.3	26.7	11.4	0.8
Commodities (naïve)	-18.9	-2.4	-36.9	18.5	-12.0
Core Private Infrastructure	-1.3	3.7	-0.8	24.8	-0.3
Hedge Funds	-9.1	-0.4	-17.8	-2.1	-9.4
Long-Short	-10.9	-1.0	-26.4	-8.8	-8.3
Hedge Fund of Funds	-7.6	-0.5	-19.5	-0.4	-7.7

Negative Historical Scenario Returns - Sample Inputs (continued)

	Rate spike (1994 Calendar Year)	Crash of 1987 (Sep - Nov 1987)	Strong dollar (Jan 1981 - Sep 1982)	Volcker Recession (Jan - Mar 1980)	Stagflation (Jan 1973 - Sep 1974)
Cash Equivalents	3.9	1.4	24.4	2.9	13.5
Short-term Investment Grade Bonds	0.5	2.3	29.9	-2.6	4.3
Investment Grade Bonds	-2.9	2.2	29.9	-8.7	7.9
Long-term Corporate Bonds	-5.8	1.5	29.6	-14.1	-12.0
Long-term Government Bonds	-7.6	2.6	28.4	-13.6	-1.8
TIPS	-7.5	2.8	15.6	-7.8	4.3
Global ILBs	-7.9	2.9	16.5	-8.3	4.5
High Yield Bonds	-1.0	-3.6	6.9	-2.3	-15.5
Bank Loans	10.3	-1.7	3.3	-1.1	-7.5
Direct Lending	7.6	-2.3	3.2	-1.0	-7.2
Foreign Bonds	5.3	-0.3	34.8	-6.5	-1.4
Asset Based Lending	7.6	-2.3	3.2	-1.0	-7.2
Special Situations	7.6	-2.3	3.2	-1.0	-7.2
Emerging Market Bonds (major)	-18.9	-9.2	-1.6	-2.6	-20.2
Emerging Market Bonds (local)	-22.8	-11.0	-2.0	-3.2	-23.9
US Equity	1.3	-29.5	-2.3	-4.1	-42.6
Developed Market Equity (non-US)	7.8	-14.5	-18.0	-7.0	-36.3
Emerging Market Equity	-7.3	-25.3	-12.1	-6.6	-44.2
Global Equity	5.0	-20.5	-11.1	-5.4	-40.4
Private Equity/Debt	13.2	-0.7	-2.7	-2.5	-18.2
Private Equity	14.2	-0.5	-3.9	-2.7	-20.1
Private Debt Composite	6.2	-1.8	3.0	-1.0	-6.9
REITs	-3.5	-19.5	2.5	-3.6	-33.9
Core Private Real Estate	6.4	2.5	23.9	5.5	-4.4
Value-Added Real Estate	6.5	4.3	44.2	9.6	-7.6
Opportunistic Real Estate	18.8	3.1	30.7	7.0	-5.6
Natural Resources (Private)	12.6	-9.9	-9.5	-9.1	19.3
Timberland	15.4	9.2	23.6	-7.4	5.5
Farmland	9.4	5.3	13.3	-4.2	3.1
Commodities (naïve)	16.6	1.8	-16.0	-9.6	139.5
Core Private Infrastructure	-11.5	-0.1	-0.2	-0.1	-0.5
Hedge Funds	4.1	-7.8	-3.8	-1.9	-15.7
Long-Short	2.6	-10.0	-4.9	-2.5	-19.8
Hedge Fund of Funds	-3.5	-5.7	-2.7	-1.4	-11.5

Positive Historical Scenario Returns - Sample Inputs

	Covid-19 Recovery (Apr 2020 – Dec 2021)	Global Financial Crisis Recover (Mar 2009 - Nov 2009)	Best of Great Moderation (Apr 2003 - Feb 2004)	Peak of the TMT Bubble (Oct 1998 - Mar 2000)	Plummeting Dollar (Jan 1986 - Aug 1987)	Volcker Recovery (Aug 1982 - Apr 1983)	Bretton Wood Recovery (Oct 1974 - Jun 1975)
Cash Equivalents	0.1	0.1	0.9	6.7	10.0	6.0	4.5
Short-term Investment Grade Bonds	1.1	4.3	2.8	5.3	13.2	15.4	5.0
Investment Grade Bonds	2.6	9.0	4.6	1.7	14.4	26.4	9.2
Long-term Corporate Bonds	18.0	28.8	11.3	-3.1	15.9	42.1	17.5
Long-term Government Bonds	-7.2	2.0	4.9	-2.3	15.4	33.6	11.8
TIPS	15.6	14.3	9.1	6.3	10.2	11.5	4.1
Global ILBs	18.9	24.7	9.6	6.6	10.8	12.1	4.3
High Yield Bonds	29.1	49.1	21.8	2.1	24.9	23.3	19.3
Bank Loans	24.8	32.9	10.1	6.1	11.1	10.4	8.7
Direct Lending	25.0	9.4	23.7	26.8	5.4	8.2	8.3
Foreign Bonds	5.2	23.4	15.2	-7.0	44.5	32.3	17.9
Asset Based Lending	25.0	9.4	23.7	26.8	5.4	8.2	8.3
Special Situations	85.8	33.2	23.7	26.8	5.4	8.2	8.3
Emerging Market Bonds (major)	15.7	27.0	20.6	49.0	38.9	21.6	21.0
Emerging Market Bonds (local)	7.0	37.5	25.2	61.0	48.4	26.5	25.7
US Equity	92.0	51.6	37.2	50.2	64.8	59.3	55.1
Developed Market Equity (non-US)	55.4	60.5	56.7	53.0	140.0	29.6	34.6
Emerging Market Equity	50.9	94.6	79.4	101.3	126.5	52.1	53.4
Global Equity	75.2	59.9	46.2	54.8	98.7	46.3	43.8
Private Equity/Debt	97.8	18.8	23.3	82.4	19.0	13.7	18.4
Private Equity	101.5	16.7	23.7	90.0	21.6	14.8	20.2
Private Debt Composite	41.2	28.7	20.4	21.3	5.9	7.9	8.0
REITs	75.1	82.5	44.6	-5.2	51.8	47.4	42.5
Core Private Real Estate	21.4	-12.1	9.0	18.1	13.1	6.8	4.5
Value-Added Real Estate	36.6	-22.4	10.9	22.0	23.6	11.9	7.8
Opportunistic Real Estate	41.1	-14.8	13.6	27.9	16.7	8.6	5.7
Natural Resources (Private)	45.4	57.6	36.1	22.2	78.3	30.2	14.8
Timberland	9.9	-3.7	8.5	20.5	28.6	20.0	8.7
Farmland	11.3	4.5	9.6	10.4	15.9	11.3	5.0
Commodities (naïve)	60.5	28.9	30.6	17.1	27.6	6.2	-20.2
Core Private Infrastructure	32.7	6.9	8.5	33.0	1.4	0.6	0.6
Hedge Funds	39.3	20.1	22.4	52.8	30.6	13.8	14.5
Long-Short	54.1	25.9	25.3	81.4	40.8	18.0	18.9
Hedge Fund of Funds	29.1	10.3	13.3	36.8	21.3	9.7	10.3

Stress Test Return Assumptions - Sample Inputs[1]

	10-year Treasury Bond rates rise 100 bps	10-year Treasury Bond rates rise 200 bps	10-year Treasury Bond rates rise 300 bps	Baa Spreads widen by 50 bps, High Yield by 200 bps	Baa Spreads widen by 300 bps, High Yield by 1000 bps	Trade Weighted Dollar gains 10%	Trade Weighted Dollar gains 20%	US Equities decline 10%	US Equities decline 25%	US Equities decline 40%
Cash Equivalents	-0.2	-0.4	-0.5	2.8	1.1	3.6	1.3	2.9	2.3	0.4
Short-term Investment Grade Bonds	-1.2	-2.5	-3.7	2.2	1.5	0.8	1.4	0.9	0.7	0.8
Investment Grade Bonds	-4.3	-8.4	-11.9	3.9	-0.4	0.8	4.2	1.5	0.7	-1.0
Long-term Corporate Bonds	-8.9	-16.3	-20.9	2.6	-13.4	-1.0	8.1	-1.0	-8.3	-12.3
Long-term Government Bonds	-10.6	-18.9	-23.6	7.8	7.3	1.8	12.8	1.4	2.6	2.4
TIPS	-4.9	-9.8	-13.7	2.8	-6.1	-2.4	-0.2	1.8	-2.3	-8.7
Global ILBs	-1.6	-8.6	-11.9	2.4	-11.1	-4.0	-4.8	1.4	-5.4	-16.3
High Yield Bonds	2.6	-4.3	-3.6	-1.8	-23.0	-4.1	-0.6	-5.3	-15.5	-21.2
Bank Loans	1.4	-1.0	-5.1	-2.8	-20.8	-2.9	-0.6	-3.6	-13.2	-17.4
Direct Lending	0.1	-2.7	-6.3	-1.8	-9.1	-3.2	-0.6	-3.4	-7.6	-5.7
Foreign Bonds	-4.6	-9.9	-15.7	6.6	-2.9	-4.5	-8.8	0.4	-4.6	-9.2
Asset-Based Lending	-0.2	-2.5	-4.5	-1.4	-11.5	-3.4	-3.1	-3.3	-8.2	-6.0
Special Situations	4.6	0.0	-6.4	-2.2	-21.4	-1.6	-9.0	-4.3	-17.3	-21.8
Emerging Market Bonds (major)	0.8	-6.1	-3.6	-0.1	-14.7	-2.6	-4.2	-4.2	-12.5	-15.4
Emerging Market Bonds (local)	1.6	-6.4	-3.0	0.1	-12.8	-3.0	-12.2	-3.8	-13.3	-20.5
US Equity	7.1	-1.0	2.8	-1.2	-32.0	-3.5	1.6	-10.6	-26.5	-42.4
Developed Market Equity (non-US)	8.9	0.7	-5.6	0.3	-35.1	-13.2	-9.0	-8.8	-23.4	-41.4
Emerging Market Equity	10.0	2.3	0.1	-1.1	-42.8	-15.7	-15.7	-11.7	-30.8	-46.9
Global Equity	7.6	-0.1	-0.5	-0.7	-33.6	-9.1	-5.9	-9.8	-25.3	-41.5
Private Equity/Debt	6.5	0.9	-5.5	-0.2	-22.5	-2.9	-7.2	-9.2	-22.5	-25.3
Private Equity	6.8	0.9	-5.3	0.0	-22.8	-2.8	-6.4	-10.0	-23.3	-25.7
Private Debt Composite	2.6	-1.3	-6.2	-1.8	-15.8	-2.4	-4.3	-4.0	-12.8	-15.0
REITs	4.1	-4.4	1.2	-3.8	-37.3	-1.6	12.4	-7.1	-32.8	-55.7
Core Private Real Estate	2.6	4.2	5.0	2.0	-7.1	2.7	9.7	1.0	-8.5	-14.0
Value-Added Real Estate	4.9	7.5	14.1	7.2	-13.5	13.7	6.4	1.9	-13.6	-23.1
Opportunistic Real Estate	4.2	6.9	9.9	1.1	-20.6	2.3	15.6	-0.6	-17.1	-26.3
Natural Resources (Private)	13.3	6.9	-3.5	-0.9	-27.5	-4.3	-21.5	-2.1	-17.0	-29.1
Timberland	1.5	2.3	-9.9	5.0	6.9	2.9	8.6	0.6	2.7	3.9
Farmland	2.5	0.7	-9.2	3.9	10.1	1.3	8.0	1.0	4.9	10.3
Commodities (naïve)	9.9	6.0	-6.6	-4.3	-25.0	-3.4	-24.0	5.1	-11.1	-37.8
Core Private Infrastructure	0.5	-4.6	-6.1	1.2	0.1	-0.7	3.6	-0.4	-5.0	-7.8
Hedge Funds	2.9	-1.8	-5.1	-0.6	-14.5	-2.2	-1.7	-4.3	-12.2	-15.7
Long-Short	5.2	-1.8	-4.2	-0.1	-21.0	-3.7	-4.3	-7.5	-17.7	-23.5
Hedge Fund of Funds	2.1	-2.4	-5.7	-1.3	-14.8	-2.9	-2.4	-4.9	-12.5	-16.0

[1] Assumptions are based on performance for each asset class during historical periods that resembled these situations.

'Anti' Stress Test Return Assumptions - Sample Inputs[1]

	10-year Treasury Bond rates drop 100 bps	10-year Treasury Bond rates drop 200 bps	Baa Spreads narrow by 30bps, High Yield by 100 bps	Baa Spreads narrow by 100bps, High Yield by 300 bps	Trade Weighted Dollar drops 10%	Trade Weighted Dollar drops 20%	US Equities rise 10%	US Equities rise 30%
Cash Equivalents	0.2	0.4	0.6	0.2	2.0	4.5	2.3	3.1
Short-term Investment Grade Bonds	1.3	2.6	0.5	2.0	1.5	3.3	0.8	1.6
Investment Grade Bonds	4.5	9.3	1.3	3.9	2.5	9.4	1.8	3.8
Long-term Corporate Bonds	10.5	23.4	3.9	14.5	5.6	15.8	3.6	7.7
Long-term Government Bonds	13.3	28.8	0.6	-0.6	1.8	22.2	3.6	5.7
TIPS	5.2	10.9	1.2	5.9	3.8	7.8	1.5	2.2
Global ILBs	3.0	6.4	2.1	7.4	5.9	8.4	1.7	3.2
High Yield Bonds	2.8	8.9	7.0	25.7	7.7	8.6	4.8	10.6
Bank Loans	-0.2	2.2	4.0	16.4	4.3	0.6	2.2	4.5
Direct Lending	-0.5	0.2	4.9	5.6	1.5	3.8	1.8	3.5
Foreign Bonds	5.7	11.3	1.6	7.4	9.9	21.3	2.3	6.8
Asset Based Lending	-0.6	1.5	3.4	4.8	1.0	5.9	1.8	5.0
Special Situations	1.2	2.9	9.5	17.1	6.8	7.8	6.2	10.0
Emerging Market Bonds (major)	3.1	7.4	5.5	15.5	7.4	15.4	5.5	11.1
Emerging Market Bonds (local)	3.7	9.9	5.5	17.6	10.5	19.4	6.1	13.2
US Equity	3.4	15.3	11.4	18.8	8.0	24.9	10.6	31.7
Developed Market Equity (non-US)	-2.4	16.4	9.4	18.3	13.4	47.6	6.4	18.8
Emerging Market Equity	0.5	17.8	9.5	34.3	20.1	47.9	9.3	28.9
Global Equity	0.7	15.2	9.6	19.6	11.3	35.9	8.6	25.7
Private Equity/Debt	2.4	4.4	10.5	9.5	7.4	16.7	10.5	13.6
Private Equity	2.5	4.3	10.6	8.3	7.3	17.3	11.1	14.3
Private Debt Composite	0.8	1.8	7.7	12.8	4.8	5.9	4.6	6.5
REITs	2.6	14.5	9.7	27.1	6.5	25.5	10.0	24.1
Core Private Real Estate	1.0	1.6	4.6	-3.5	1.2	5.5	3.0	3.6
Value-Added Real Estate	2.7	6.4	5.6	-9.4	0.9	12.6	6.0	7.4
Opportunistic Real Estate	0.1	3.9	5.9	-5.5	-0.4	11.4	4.7	6.2
Natural Resources (Private)	-1.1	11.3	10.2	31.0	16.9	27.2	7.6	15.0
Timberland	6.4	9.2	4.9	-0.6	3.8	12.9	6.4	5.5
Farmland	3.2	4.2	6.6	3.8	3.4	7.8	5.3	4.1
Commodities (naïve)	-2.6	-3.2	3.1	9.8	13.6	-2.5	3.1	4.0
Core Private Infrastructure	0.8	-4.3	7.0	4.8	3.5	-2.3	2.0	2.9
Hedge Funds	3.3	4.8	5.8	11.3	6.0	9.3	5.6	9.8
Long-Short	3.3	5.8	6.9	12.3	7.8	15.2	7.0	13.3
Hedge Fund of Funds	2.5	3.9	4.9	10.2	5.1	8.3	4.7	8.8

[1] Assumptions are based on performance for each asset class during historical periods that resembled these situations.

Inflation Scenario Description

Scenario	Scenario Description
Inflation slightly higher than expected	Inflation is .05% above inflation expectation (i.e. surprise inflation is .05%). .05% is the 25th percentile of positive, historical surprise inflation.
Inflation moderately higher than expected	Inflation is .15% above inflation expectation (i.e. surprise inflation is .15%). .15% is the median of positive, historical surprise inflation.
Inflation meaningfully higher than expected	Inflation is .3% above inflation expectation (i.e. surprise inflation is .3%). .3% is the 75th percentile of positive, historical surprise inflation.
High Growth and Low Inflation	The real GDP growth rate is 1% and inflation is .07%. 1% GDP growth is the 75th percentile of historical GDP growth and .07% inflation is the 25th percentile of historical inflation.
High Growth and Moderate Inflation	The real GDP growth rate is 1% and inflation is .25%. 1% GDP growth is the 75th percentile of historical GDP growth and .25% inflation is the median of historical inflation.
High Growth and High Inflation	The real GDP growth rate is 1% and inflation is .5%. 1% GDP growth is the 75th percentile of historical GDP growth and .5% inflation is the 75th percentile of historical inflation.
Low Growth and Low Inflation	The real GDP growth rate is .3% and inflation is .07%. .3% GDP growth is the 25th percentile of historical GDP growth and .07% inflation is the 25th percentile of historical inflation.
Low Growth and Moderate Inflation	The real GDP growth rate is .3% and inflation is .25%. .3% GDP growth is the 25th percentile of historical GDP growth and .25% inflation is the median of historical inflation.
Low Growth and High Inflation	The real GDP growth rate is .3% and inflation is .5%. .3% GDP growth is the 25th percentile of historical GDP growth and .5% inflation is the 75th percentile of historical inflation.
Very brief, moderate inflation spike	Inflation is .45% and lasts for 1-2 months. .45% is the 75th percentile of historical inflation.
Brief, moderate inflation spike	Inflation is .45% and lasts for 4-8 months. .45% is the 75th percentile of historical inflation.
Extended, moderate inflation spike	Inflation is .45% and lasts for 12+ months. .45% is the 75th percentile of historical inflation.
Very brief, extreme inflation spike	Inflation is .9% and lasts for 1-2 months. .9% is the 95th percentile of historical inflation.
Brief, extreme inflation spike	Inflation is .9% and lasts for 4-8 months. .9% is the 95th percentile of historical inflation.
Extended, extreme inflation spike	Inflation is .9% and lasts for 12+ months. .9% is the 95th percentile of historical inflation.

Notes and Disclaimers

[1] The returns shown in the Policy Options and Risk Analysis sections rely on estimates of expected return, standard deviation, and correlation developed by Meketa Investment Group. To the extent that actual return patterns to the asset classes differ from our expectations, the results in the table will be incorrect. However, our inputs represent our best unbiased estimates of these simple parameters.

[2] The returns shown in the Policy Options and Risk Analysis sections use a lognormal distribution, which may or may not be an accurate representation of each asset classes' future return distribution. To the extent that it is not accurate in whole or in part, the probabilities listed in the table will be incorrect. As an example, if some asset classes' actual distributions are even more right-skewed than the lognormal distribution (i.e., more frequent low returns and less frequent high returns), then the probability of the portfolio hitting a given annual return will be lower than that stated in the table.

[3] The standard deviation bars in the chart in the Risk Analysis section do not indicate the likelihood of a 1, 2, or 3 standard deviation event—they simply indicate the return we expect if such an event occurs. Since the likelihood of such an event is the same across allocations regardless of the underlying distribution, a relative comparison across policy choices remains valid.

2024 Capital Market Expectations

Executive Summary

→ 2023 was a volatile year for most investors, but ultimately most asset classes experienced positive returns, including double-digit gains for many risky assets.

→ With the notable exception of China's markets, global bond and equity markets rallied at the end of the year, posting strong gains as inflation pressures eased and central banks appeared to be turning away from tightening policies.

- Despite short-term interest rates climbing, the yield on most Treasury bonds finished the year near where they started it.
- Credit spreads tightened, especially for lower quality credit such as high yield. The result is lower expected returns for many credit-oriented assets.
- Most equity markets rallied in 2023, generally at a much faster pace than the gain in earnings. Hence many equity markets were trading at higher valuations at year-end, thus reducing their forward-looking returns.

→ Our 10-year CMEs continue to be lower than our 20-year CMEs for the vast majority of asset classes, partly due to a higher assumed "risk-free" rate in the future.

→ The net result is a meaningful decrease in return assumptions for most assets over the 10-year horizon, with much more mixed and modest changes at the 20-year horizon.

Setting Capital Market Expectations

→ Capital markets expectations (CMEs) are the inputs needed to determine the long-term risk and returns expectations for a portfolio.

- They serve as the starting point for determining asset allocation.

→ Consultants (including Meketa) generally set them once a year.

- Our results are published in January and based on data as of December 31 for public markets and September 30 for private markets.
- Changes are driven by many factors, including interest rates, credit spreads, cap rates, and equity prices.

→ Setting CMEs involves crafting long-term forecasts for:

- Returns
- Standard Deviation
- Correlations (i.e., covariance)

→ Our process relies on both quantitative and qualitative methodologies.

Building 10-year Forecasts

→ Our first step is to develop 10-year forecasts based on fundamental models.

- Each model is based on the most important factors that drive returns for that asset class:

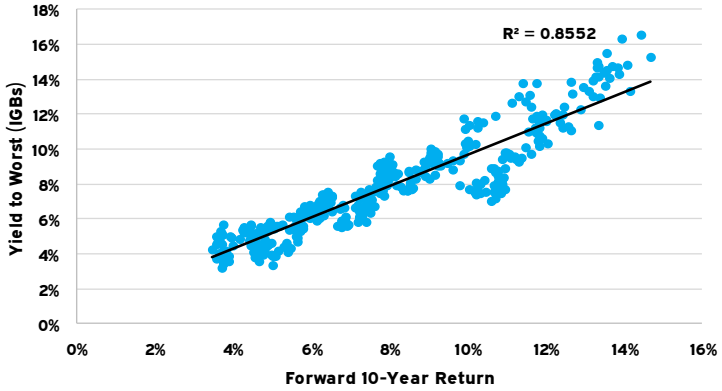
Asset Class Category	Major Factors
Equities	Dividend Yield, GDP Growth, Valuation
Bonds	Yield to Worst, Default Rate, Recovery Rate
Commodities	Collateral Yield, Roll Yield, Inflation
Infrastructure	Public IS Valuation, Income, Growth, Leverage
Natural Resources	Price per Acre, Income, Public Market Valuation
Real Estate	Cap Rate, Yield, Growth, Leverage
Private Equity	EBITDA Multiple, Leverage, Public VC Valuation
Hedge Funds and Other	Leverage, Alternative Betas

→ The common components are income, growth, and valuation.

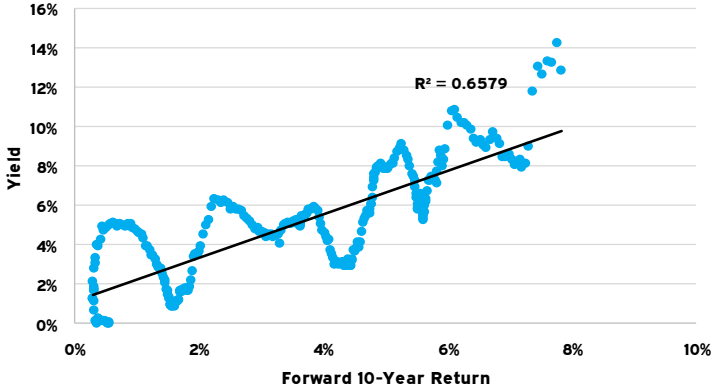
- Leverage and currency impact are also key factors for many strategies.

Some factors are naturally more predictive than others

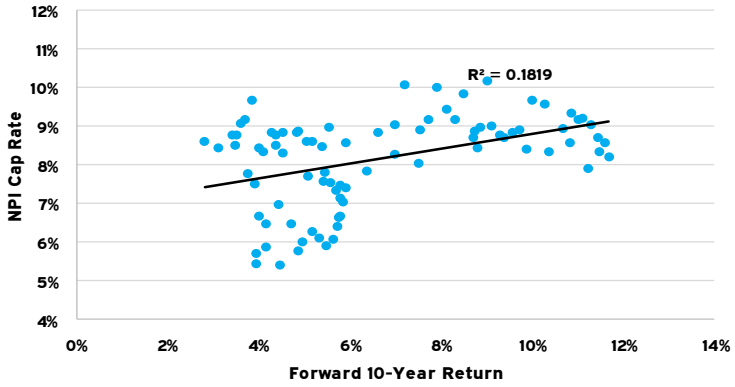
Investment Grade Bonds
Yield to Worst vs. Forward 10-Year Returns



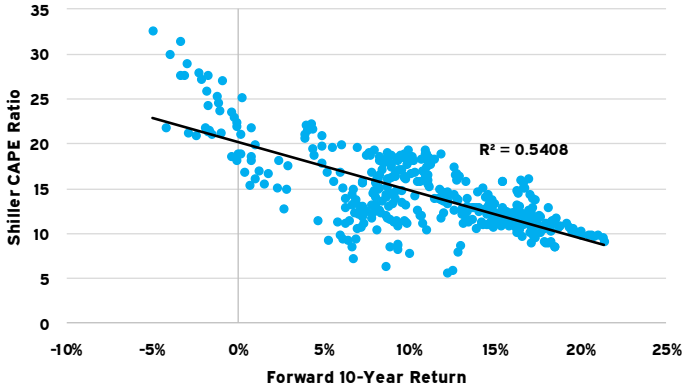
Cash (90-day T-Bill)
Yield vs. Forward 10-Year Returns



Core Real Estate
Cap Rates vs. Forward 10-Year Returns



US Equities
Shiller CAPE vs. Forward 10-Year Returns



Sources: Bloomberg, FRED, NCREIF, S&P, Robert Shiller (Yale University), and Meketa Investment Group. As of December 31, 2022.

10-year Model Example: Bonds

→ The short version for investment grade bond models is:

$$E(R) = \text{Current YTW (yield to worst)}$$

→ Our models assume that there is a reversion to the mean for spreads (though not yields).

→ For TIPS, we add the real yield of the TIPS index to the breakeven inflation rate.

→ As with equities, we make currency adjustments when necessary for foreign bonds.

→ For bonds with credit risk, Meketa Investment Group estimates default rates and loss rates in order to project an expected return:

$$E(R) = YTW - (\text{Annual Default Rate} \times \text{Loss Rate})$$

10-year Model Example: Equities

→ We use a fundamental model for equities that combines income and capital appreciation.

$$E(R) = \text{Dividend Yield} + \text{Expected Earnings Growth} + \text{Multiple Effect} + \text{Currency Effect}$$

→ Meketa evaluates historical data to develop expectations for dividend yield, earnings growth, the multiple effect, and currency effect.

- Earnings growth is a function of real GDP growth, inflation, and exposure to foreign revenue sources.
- We assume that long-term earnings growth is linked to economic growth.
- However, many factors can cause differences between economic growth and EPS growth.

→ Our models assume that there is a reversion toward mean pricing over this time frame.

Moving from 10-Year to 20-Year Forecasts

→ Our next step is to combine our 10-year forecasts with projections for years 11-20 for each asset class.

→ We use a risk premia approach to forecast 10-year returns in ten years (i.e., years 11-20).

- We start with an assumption (market informed, such as the 10-year forward rate) for what the risk-free rate will be in ten years.
- We then add a risk premia for each asset class.
- We use historical risk premia as a guide, but many asset classes will differ from this, especially if they have a shorter history.
- We seek consistency with finance theory (i.e., riskier assets will have a higher risk premia assumption).

→ Essentially, we assume mean-reversion over the first ten years (where appropriate), and consistency with CAPM thereafter.

→ The final step is to make any qualitative adjustments.

- The Investment Policy Committee reviews the output and may make adjustments.

The Other Inputs: Standard Deviation and Correlation

→ Standard deviation:

- We review the trailing twenty-year standard deviation, as well as skewness.
- Historical standard deviation serves as the base for our assumptions.
- If there is a negative skew, we increased the volatility assumption based on the size of the historical skewness.

Asset Class	Historical Standard Deviation (%)	Skewness	Assumption[1] (%)
Bank Loans	6.5	-2.9	10.0
FI / L-S Credit	5.8	-2.7	9.0

- We also adjust for private market asset classes with "smoothed" return streams.

→ Correlation:

- We use trailing twenty-year correlations as our guide.
- Again, we make adjustments for "smoothed" return streams.

→ Most of our adjustments are conservative in nature (i.e., they increase the standard deviation and correlation).

[1] Note that we round our standard deviation assumptions to whole numbers.

Similar or Lower Yields

→ Short-term interest rates are higher than one year ago, while the 10-year Treasury yield ended the year where it started it.

→ Similar levels of interest rates combined with tighter credit spreads to result in slightly lower yields for most sectors of the global bond market.

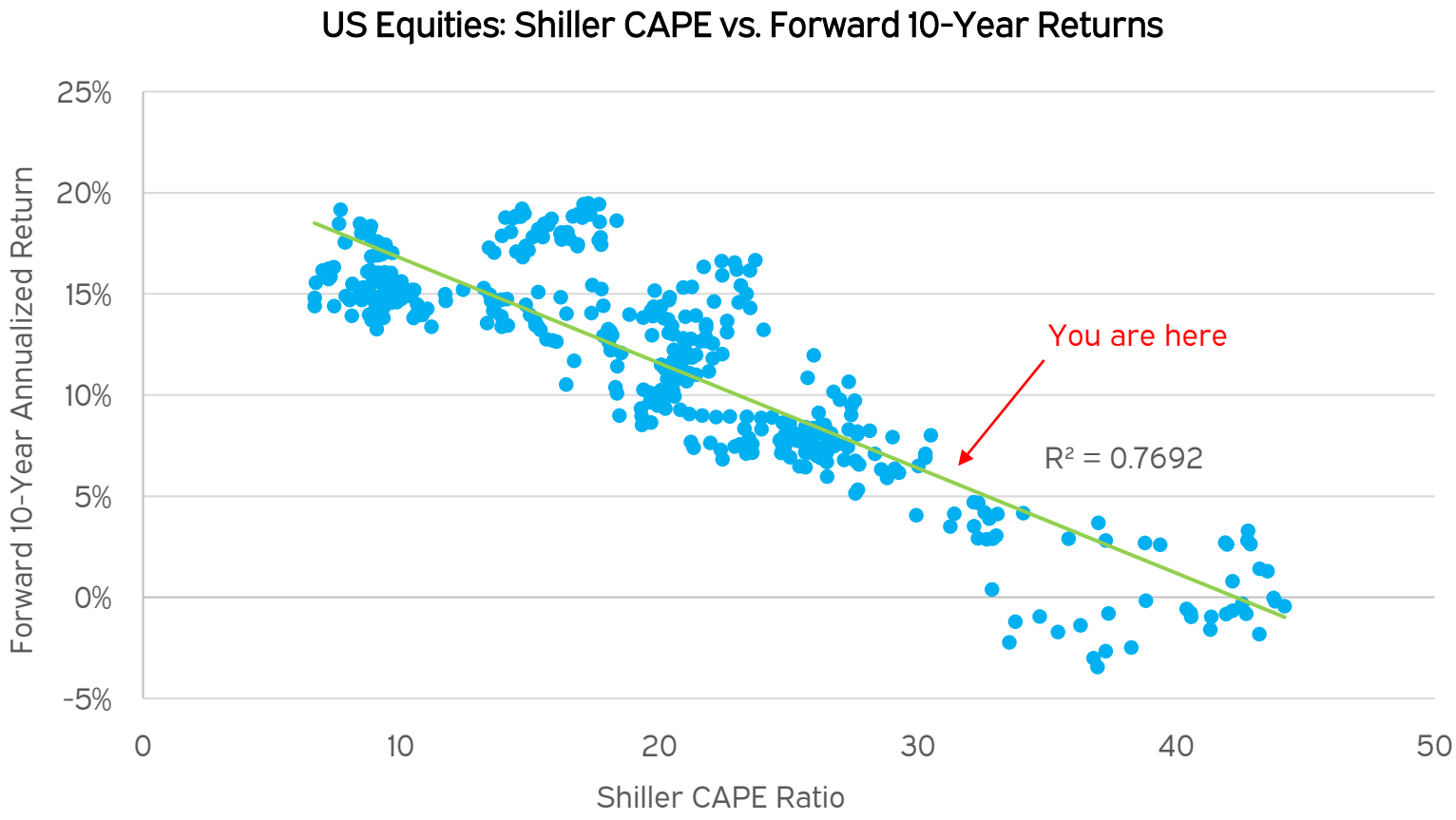
Index	Yield to Worst 12/31/23 (%)	Yield to Worst 12/31/22 (%)
Fed Funds Rate	5.25-5.50	4.25-4.50
10-year Treasury	3.88	3.88
Bloomberg Aggregate	4.53	4.68
Bloomberg Corporate	5.06	5.42
Bloomberg Securitized	4.72	4.75
Bloomberg Global Aggregate	3.51	3.73
Bloomberg EM Local Currency Government	4.08	4.42
Bloomberg EM Hard Currency Aggregate	6.77	7.26
Bloomberg US Corporate High Yield	7.59	8.96

Source: Bloomberg. Data is as of December 31, 2023 and December 31, 2022.

Impact of Equity Prices on Returns

→ Relative prices have been indicative of future equity returns.

→ Higher prices have led to lower future returns, and vice versa.



Source: Robert Shiller, Yale University, and Meketa Investment Group. Data is based on monthly returns and Cyclically Adjusted P/E ratio on S&P 500 Index for the period from January 1980 through December 2023.

20-year Geometric Expected Returns
Rate Sensitive

	2024 E(R) (%)	2023 E(R) (%)	Δ From 2023 (%)	Notes
Cash Equivalents	2.5	2.9	-0.4	Lower projected short-term rates
Short-term Investment Grade Bonds	3.7	3.5	0.2	
Investment Grade (Core) Bonds	4.8	4.7	0.1	
Intermediate Government Bonds	4.1	3.7	0.4	Slightly higher yields
Long-term Government Bonds	5.0	5.0	0.0	
Mortgage Backed Securities	4.9	4.6	0.3	
Investment Grade Corporate Bonds	5.4	5.4	0.0	
Long-term Corporate Bonds	6.0	5.7	0.3	
Short-term TIPS	3.7	3.6	0.1	
TIPS	4.7	4.5	0.2	
Long-term TIPS	5.2	5.2	0.0	
Global ILBs	4.7	4.7	0.0	
Foreign Bonds	3.9	4.0	-0.1	Slightly lower yields
US Inflation	*2.8*	*2.6*	*0.2*	Higher long-term inflation expectations

20-year Geometric Expected Returns
Credit

	2024 E(R) (%)	2023 E(R) (%)	Δ From 2023 (%)	Notes
High Yield Bonds	6.8	7.3	-0.5	Tighter spreads
Higher Quality High Yield	6.4	6.7	-0.3	Tighter spreads
Bank Loans	6.6	7.0	-0.4	Tighter spreads
Collateralized Loan Obligations (CLOs)	7.2	7.2	0.0	
Convertible Bonds	6.2	6.4	-0.2	Tighter spreads
Emerging Market Bonds (major)	6.8	6.4	0.4	Higher yields
Emerging Market Bonds (local)	6.2	6.0	0.2	
Private Debt	9.2	9.0	0.2	
Direct Lending	8.4	8.3	0.1	Lower assumed leverage
Asset Based Lending	9.4	9.0	0.4	Lower average fees
Special Situations Lending	9.9	10.2	-0.3	Less extreme distressed pricing

20-year Geometric Expected Returns
Equities

	2024 E(R) (%)	2023 E(R) (%)	Δ From 2023 (%)	Notes
US Equity	8.5	8.7	-0.2	Higher valuations
US Small Cap	9.4	9.3	0.1	
Developed Non-US (EAFE) Equity	8.9	9.8	-0.9	Higher valuations, lower projected earnings growth
Dev. Non-US Small Cap	9.5	10.1	-0.6	Higher valuations
Emerging Market Equity	8.9	10.0	-1.1	Higher valuations, lower projected earnings growth
Emerging Market Small Cap	8.9	10.0	-1.1	Higher valuations, lower dividend yields
Emerging Market ex-China	9.0	10.3	-1.3	Higher valuations, lower projected earnings growth
China Equity	8.6	9.3	-0.7	Lower projected earnings growth
Frontier Market Equity	10.0	10.7	-0.7	Higher valuations, lower projected growth & dividends
Global Equity	8.7	9.2	-0.5	Higher valuations
Low Volatility Equity	7.8	8.3	-0.5	Higher valuations
Private Equity	11.2	11.0	0.2	Mixed valuations and slightly lower borrowing costs
Buyouts	10.8	10.7	0.1	Mixed valuations and slightly lower borrowing costs
Growth Equity	11.5	11.2	0.3	Mixed valuations and slightly lower borrowing costs
Venture Capital	12.0	11.6	0.4	Lower valuations

20-year Geometric Expected Returns
Real Estate & Infrastructure

	2024 E(R) (%)	2023 E(R) (%)	Δ From 2023 (%)	Notes
Real Estate	8.0	7.8	0.2	Higher cap rates
US REITs	7.8	8.0	-0.2	Lower yields
Core Private Real Estate	6.9	6.5	0.4	Higher cap rates
Value-Added Real Estate	9.0	8.3	0.7	Higher cap rates
Opportunistic Real Estate	10.3	9.6	0.7	Higher cap rates
Infrastructure	9.0	8.3	0.7	Lower borrowing costs, model changes
Infrastructure (Public)	9.1	8.8	0.3	
Infrastructure (Core Private)	8.0	7.8	0.2	
Infrastructure (Non-Core Private)	10.0	9.5	0.5	Lower borrowing costs

20-year Geometric Expected Returns
Natural Resources & Commodities

	2024 E(R) (%)	2023 E(R) (%)	Δ From 2023 (%)	Notes
Natural Resources	9.3	NA		90% private, 10% public
Natural Resources (Public)	9.2	8.7	0.5	Improved relative valuations
Natural Resources (Private)	9.3	9.8	-0.5	Higher valuations
Energy	10.4	10.4	0.0	
Mining	9.9	10.2	-0.3	Higher valuations
Timberland	7.3	7.4	-0.1	
Farmland	7.0	6.5	0.5	Improved valuations, higher income expectations
Sustainability	10.0	10.3	-0.3	Higher valuations
MLPs	8.4	7.4	1.0	Improved relative valuations
Gold Mining	9.5	9.7	-0.2	Higher valuations
Gold (Metal)	3.5	3.3	0.2	Slightly higher long-term inflation expectations
Commodities	5.3	5.7	-0.4	Lower cash yield

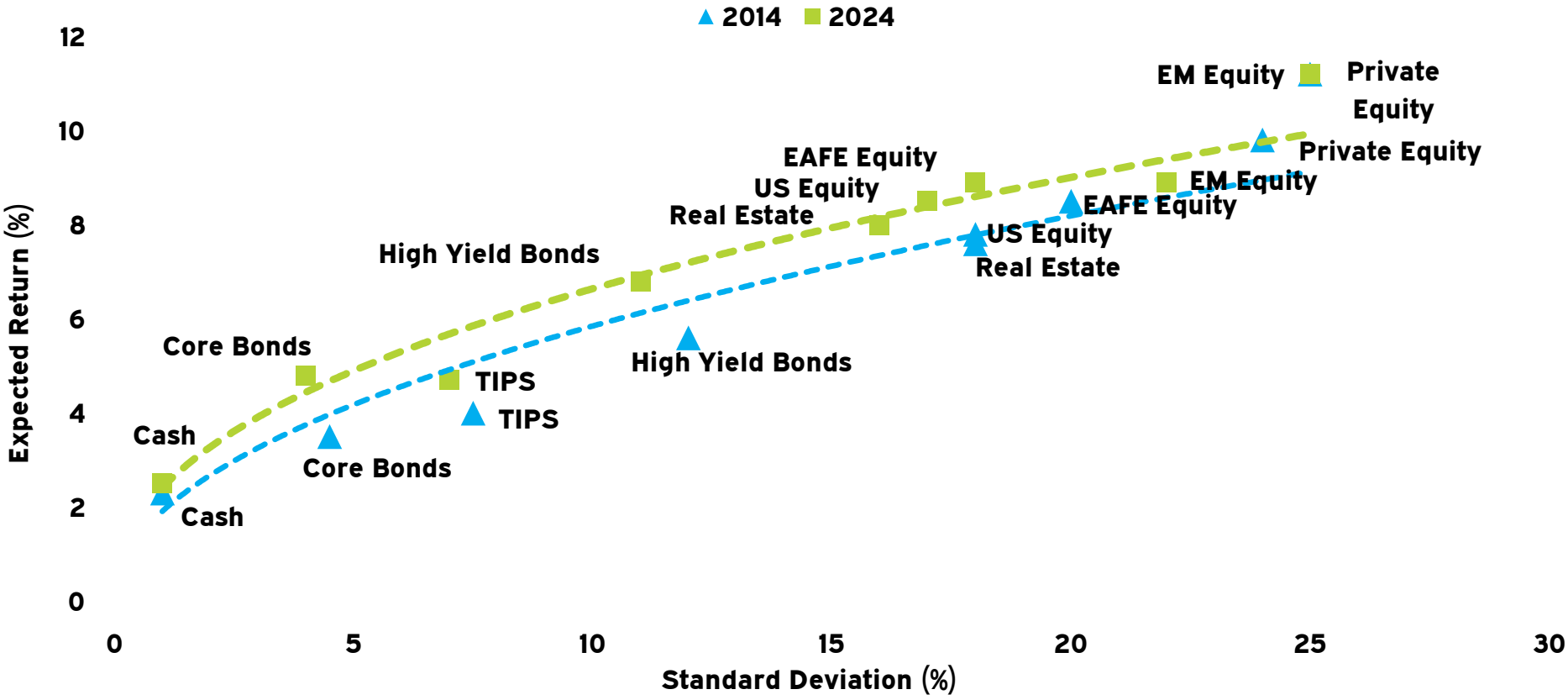
20-year Geometric Expected Returns
Alternative Strategies (Other)

	2024 E(R) (%)	2023 E(R) (%)	Δ From 2023 (%)	Notes
Hedge Funds	5.8	6.1	-0.3	Lower cash/credit yield, higher equity valuations
Long-Short	5.3	5.6	-0.3	Higher valuations, lower projected cash yield
Event Driven	7.6	7.7	-0.1	Higher valuations, lower projected cash yield
Global Macro	5.4	5.7	-0.3	Higher valuations, lower cash yield, tighter spreads
CTA – Trend Following	4.7	4.8	-0.1	
Fixed Income/L-S Credit	6.1	6.5	-0.4	Tighter spreads
Relative Value/Arbitrage	6.5	6.7	-0.2	Lower projected cash yield
Long Vol	1.2	1.1	0.1	
Insurance Linked Strategies	6.2	6.2	0.0	
Alternative Risk Premia	5.2	5.6	-0.4	Lower projected cash yield
Risk Parity (10% vol)	7.2	7.7	-0.5	Higher equity valuations, tighter credit spreads
TAA	6.1	5.7	0.4	Model changes
Digital Currencies	3.5	3.3	0.2	

The Big Picture: Higher Return for Similar Risk[1]

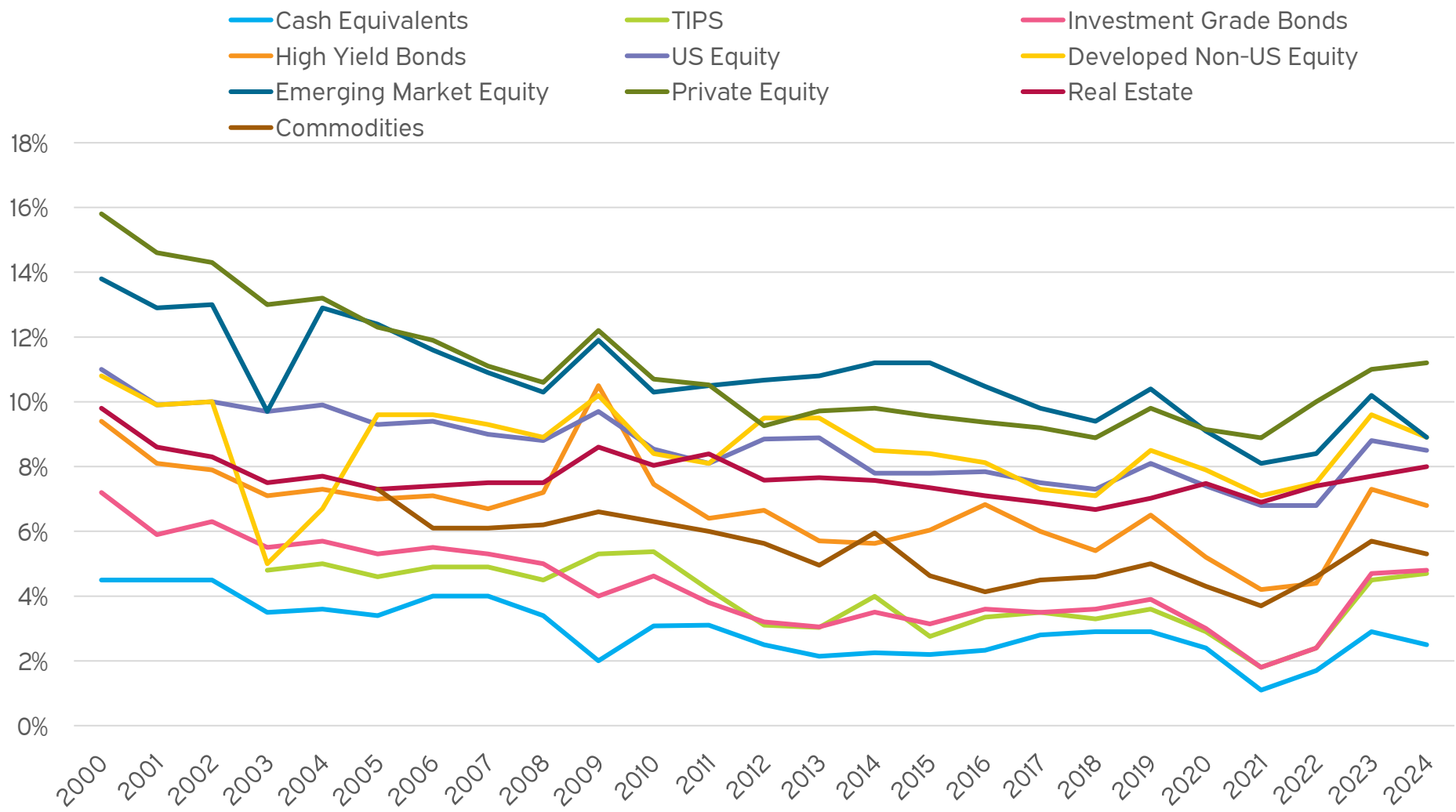
→ The relationship between long-term return expectations and the level of risk accepted is not static.

→ The higher interest rates of the last two years mean that many investors should be able to take on less risk than they have over the past decade if they want to achieve their target returns.



[1] Expected return and standard deviation are based upon Meketa Investment Group's 2014 and 2024 20-year capital market expectations.

Our 20-year CMEs since 2000



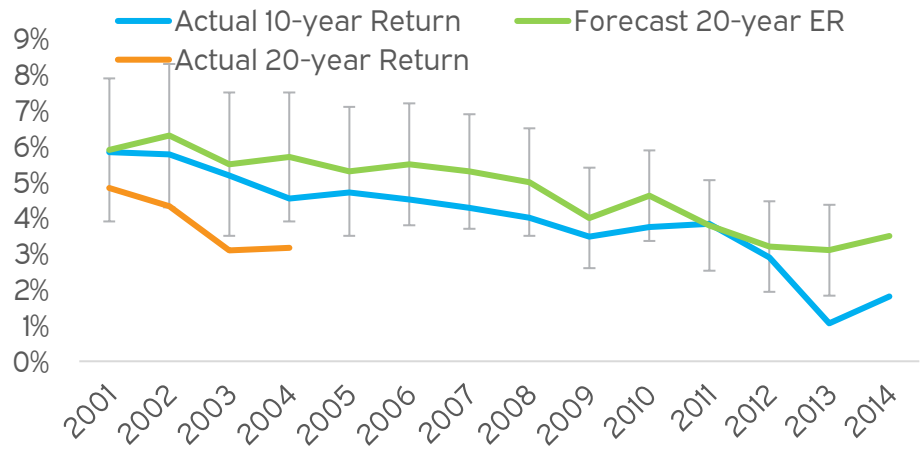
Return and Risk Data

Asset Class	10-year Expected Return (%)	20-year Expected Return (%)	Standard Deviation (%)	11-20 year Risk Premia[1] (%)
Cash Equivalents	2.4	2.5	1.0	-2.0
Investment Grade Bonds	4.6	4.8	4.0	0.4
Long-term Government Bonds	4.3	5.0	12.0	1.0
TIPS	4.3	4.7	7.0	0.4
High Yield Bonds	6.5	6.8	11.0	2.5
Bank Loans	6.5	6.6	10.0	2.0
Emerging Market Debt (local)	6.3	6.2	12.0	1.5
Private Debt	9.2	9.2	15.0	4.6
US Equity	6.9	8.5	17.0	5.5
Developed Non-US Equity	7.7	8.9	18.0	5.4
Emerging Non-US Equity	7.6	8.9	22.0	5.5
Global Equity	7.2	8.7	17.0	5.5
Private Equity	9.9	11.2	25.0	7.8
Real Estate	6.3	8.0	16.0	5.3
Infrastructure	7.4	9.0	18.0	6.1
Commodities	4.9	5.3	17.0	1.0
Hedge Funds	4.5	5.8	7.0	2.5
Inflation	2.4	2.8		-1.5

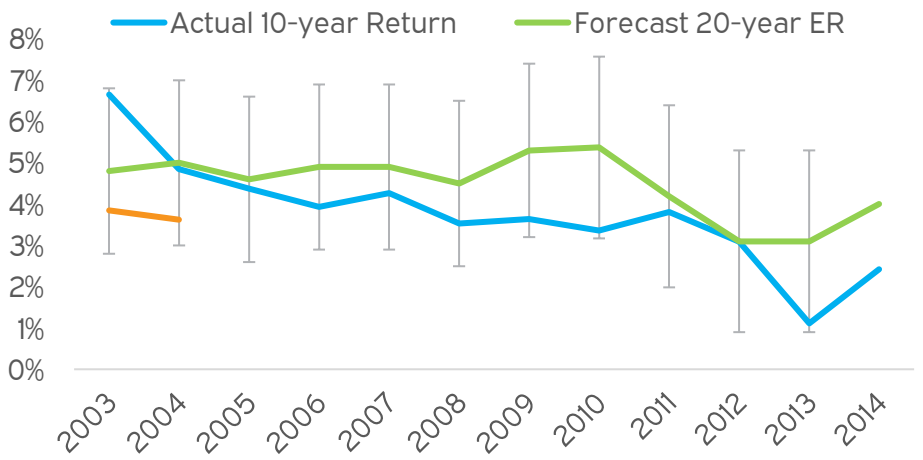
[1] Risk Premia are calculated relative to the market's projection for the yield on the 10-year Treasury in ten years..

Our Track Record

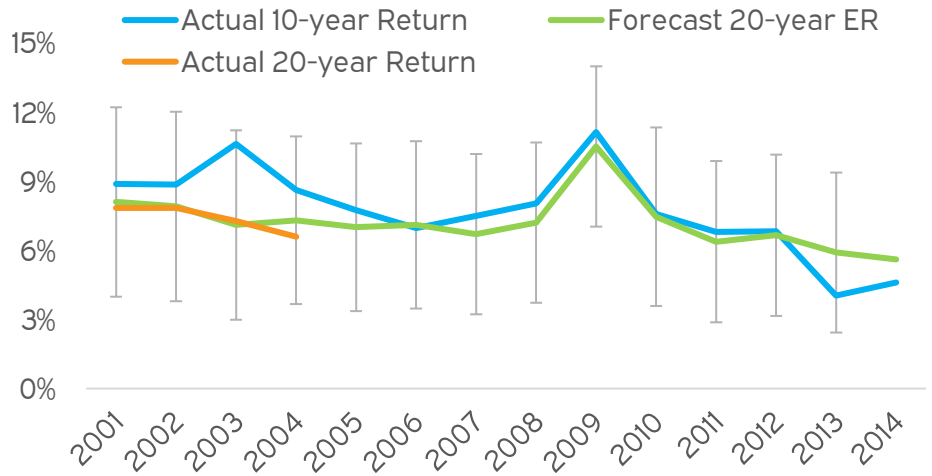
Investment Grade Bonds



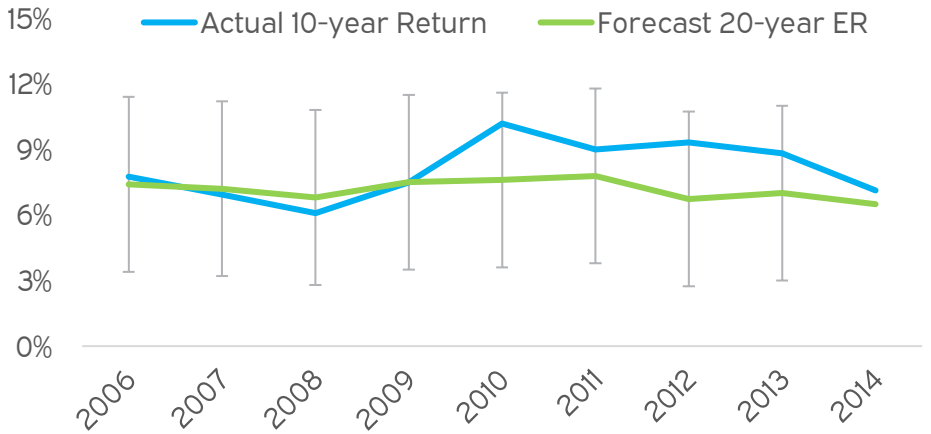
TIPS



High Yield Bonds



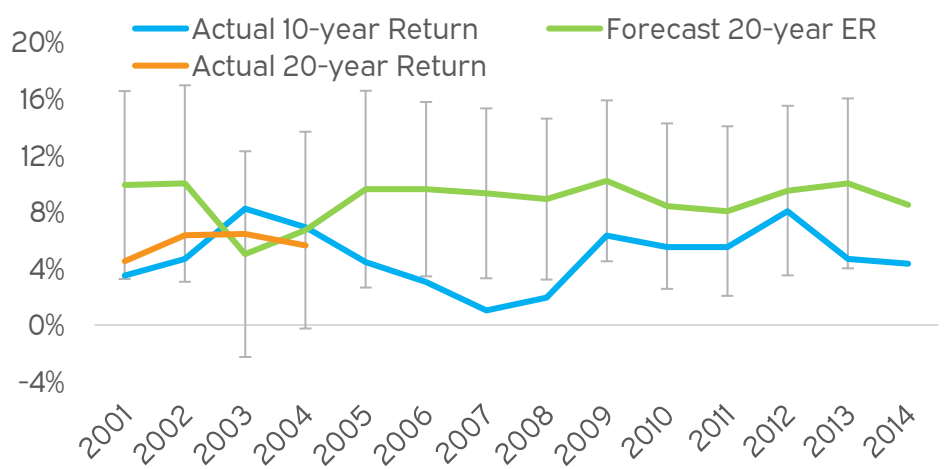
Core Real Estate



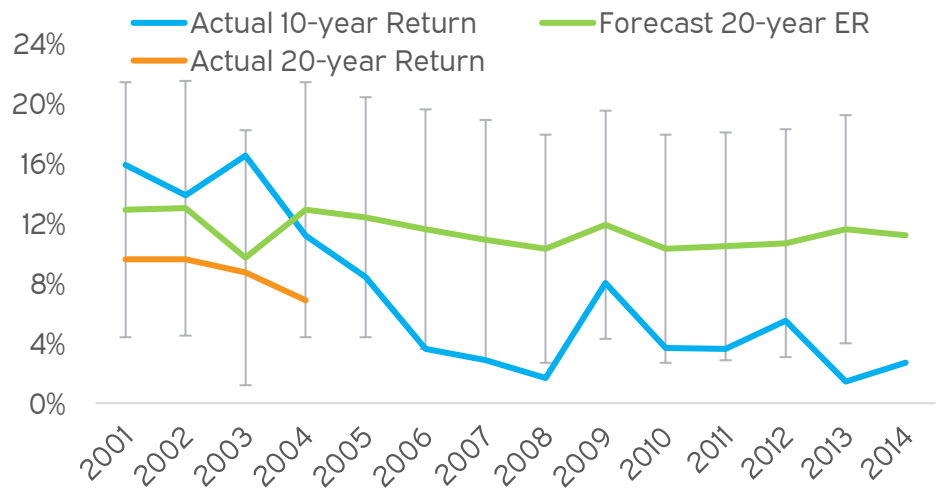
Our Track Record (continued)

US Equity

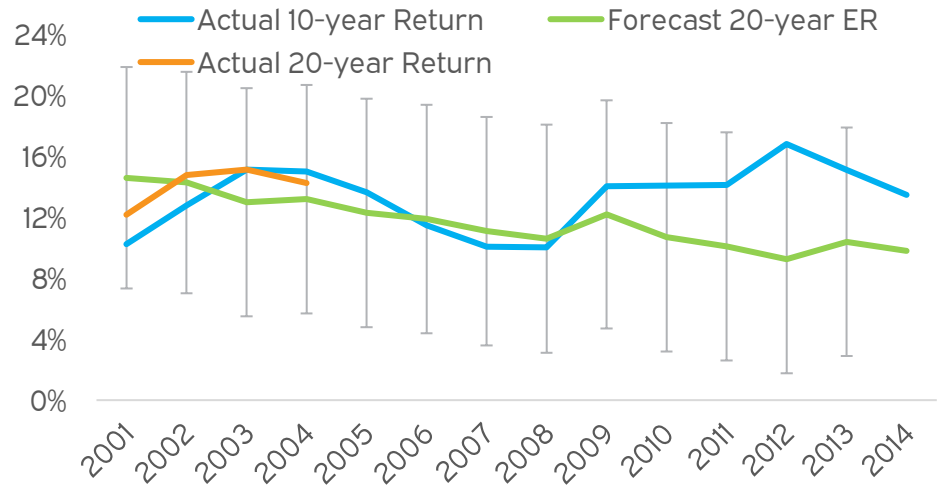
EAFE Equity



Emerging Markets Equity



Private Equity



2023 Peer Survey

→ Annually, Horizon Actuarial Services, LLC publishes a survey of capital market assumptions that they collect from various investment advisors.[1]

→ The Horizon survey is a useful tool to determine whether a consultant's expectations for returns (and risk) are reasonable.

Asset Class	Horizon 10-Year Average (%)	Meketa 10-Year (%)	Horizon 20-Year Average (%)	Meketa 20-Year (%)
Cash Equivalents	3.4	3.1	3.2	2.9
TIPS	4.1	4.3	4.1	4.5
US Core Bonds	4.7	4.8	4.8	4.7
US High Yield Bonds	6.4	8.0	6.5	7.3
Emerging Market Debt	6.3	6.5	6.4	6.2
Private Debt	8.2	9.4	8.2	9.0
US Equity (large cap)	6.9	7.8	7.4	8.7
Developed Non-US Equity	7.5	10.1	7.8	9.8
Emerging Non-US Equity	8.2	10.3	8.6	10.0
Private Equity	9.5	9.7	10.1	11.0
Real Estate	6.0	5.9	6.3	7.8
Infrastructure	7.0	6.9	7.1	8.3
Commodities	5.0	6.3	4.9	5.7
Hedge Funds	6.0	5.4	6.2	6.1
Inflation	2.6	2.5	2.5	2.6

[1] The 10-year horizon included all 42 respondents to the survey, and the 20-year horizon included 27 respondents. Figures are based on Meketa's 2023 CMEs.

WE HAVE PREPARED THIS REPORT (THIS "REPORT") FOR THE SOLE BENEFIT OF THE INTENDED RECIPIENT (THE "RECIPIENT").

SIGNIFICANT EVENTS MAY OCCUR (OR HAVE OCCURRED) AFTER THE DATE OF THIS REPORT AND THAT IT IS NOT OUR FUNCTION OR RESPONSIBILITY TO UPDATE THIS REPORT. ANY OPINIONS OR RECOMMENDATIONS PRESENTED HEREIN REPRESENT OUR GOOD FAITH VIEWS AS OF THE DATE OF THIS REPORT AND ARE SUBJECT TO CHANGE AT ANY TIME. ALL INVESTMENTS INVOLVE RISK. THERE CAN BE NO GUARANTEE THAT THE STRATEGIES, TACTICS, AND METHODS DISCUSSED HERE WILL BE SUCCESSFUL.

INFORMATION USED TO PREPARE THIS REPORT WAS OBTAINED FROM INVESTMENT MANAGERS, CUSTODIANS, AND OTHER EXTERNAL SOURCES. WHILE WE HAVE EXERCISED REASONABLE CARE IN PREPARING THIS REPORT, WE CANNOT GUARANTEE THE ACCURACY OF ALL SOURCE INFORMATION CONTAINED HEREIN.

CERTAIN INFORMATION CONTAINED IN THIS REPORT MAY CONSTITUTE "FORWARD - LOOKING STATEMENTS," WHICH CAN BE IDENTIFIED BY THE USE OF TERMINOLOGY SUCH AS "MAY," "WILL," "SHOULD," "EXPECT," "AIM", "ANTICIPATE," "TARGET," "PROJECT," "ESTIMATE," "INTEND," "CONTINUE" OR "BELIEVE," OR THE NEGATIVES THEREOF OR OTHER VARIATIONS THEREON OR COMPARABLE TERMINOLOGY. ANY FORWARD-LOOKING STATEMENTS, FORECASTS, PROJECTIONS, VALUATIONS, OR RESULTS IN THIS PRESENTATION ARE BASED UPON CURRENT ASSUMPTIONS. CHANGES TO ANY ASSUMPTIONS MAY HAVE A MATERIAL IMPACT ON FORWARD - LOOKING STATEMENTS, FORECASTS, PROJECTIONS, VALUATIONS, OR RESULTS. ACTUAL RESULTS MAY THEREFORE BE MATERIALLY DIFFERENT FROM ANY FORECASTS, PROJECTIONS, VALUATIONS, OR RESULTS IN THIS PRESENTATION.

PERFORMANCE DATA CONTAINED HEREIN REPRESENT PAST PERFORMANCE. PAST PERFORMANCE IS NO GUARANTEE OF FUTURE RESULTS.

MEKETA
INVESTMENT GROUP

2175 NW Raleigh Street
Suite 300A
Portland, OR 97210

503.226.1050
Meketa.com

MEMORANDUM

TO: MercedCERA Board of Trustees
FROM: Mika Malone, Paola Nealon, David Sancewich, Inwoo Hwang, Meketa Investment Group
DATE: February 22, 2024
RE: Statement of Investment Beliefs For Discussion - **DRAFT**

Summary

The adoption of Investment Beliefs among public pension plans, particularly larger ones, has become increasingly popular as more institutional investors recognize the importance of having a clear and transparent framework to guide their investment decision processes. Meketa first introduced the concept of establishing investment beliefs in early December of 2023. In January, MercedCERA Trustee's completed a risk survey, aimed to inform and assess each individual's risk appetite as it pertains to the Asset Allocation process and management of the MercedCERA's roughly $1.2 billion plan. The attached drafted set of Investment Beliefs Statement represents a preliminary version of Meketa's effort to reflect Trustees' views. It is intended to be a discussion item only. The goal today is to discuss and debate these beliefs, and ultimately to provide guidance to Meketa as to whether some, or all of the proposed Beliefs, should be incorporated into the Investment Policy Statement (IPS).

Implementing a statement of investment beliefs for MercedCERA could serve several important purposes. These include:

Clarity and Alignment: A clear and articulated set of beliefs help guide the investment decision-making process, ensuring all stakeholders are aligned on the fundamental principles governing the Plan.

Long-term Focus: Crucial to meeting long-term pension obligations, belief statements typically emphasize a long-term investment horizon and prioritization of this perspective can be clearly captured within the document.

Risk Management: Explicitly capturing the Trustees' views toward risk and return tradeoffs and the Plan's risk management approach.

Asset Allocation Guidance: Investment Beliefs Statements often inform asset allocation decisions by outlining certain views on various asset classes, market dynamics, and investment strategies. As we kick-off the Asset Allocation Phase I today, this exercise is not only timely, but should help inform decisions around the asset Allocation review.

While investment beliefs provide a foundational framework for how decisions are made and how the Plan is managed, we also recognize that markets are dynamic, and thus Trustees' views may evolve. An investment beliefs statement should be viewed not as a static document, and instead allow for flexibility and adaptation as part of a regular review of the Investment Policy Statement.

If you have any questions, please feel free to contact us at (971) 200-3012.

MLM/PN/IH/

Statement of Investment Beliefs

DRAFT February 2024

Investment Beliefs represent the consensus views of the Trustees, as of the date of publication. They represent neither policy, nor a procedural document. Rather, they are designed to assist in framing decision making as it relates to adopting policies, selecting investments, and setting expectations with respect to its various vendors.

1. Asset allocation is a primary driver of returns
2. A long time horizon is appropriate when thinking about the portfolio's risk tolerance and return objective.
3. Volatility in the short term can be substantial, but diminishes over longer periods of time.
4. Certain segments of the capital markets have inefficiencies that can be exploited through active management.
5. The power of capital preservation is substantial. Managing short-term drawdown risk can positively impact the Fund's ability to achieve its objectives.
6. Rebalancing the portfolio is a key aspect of prudent long-term strategic asset allocation policy.
7. A disciplined execution of the long-term strategic allocation plan, rather than timing the market, is critical for the Fund's success.
8. Diversification enhances risk-adjusted returns over the long-term.
9. As a long-term investor, the illiquidity premium in private markets can be captured to enhance return potential.
10. Shifting asset allocation away from policy (i.e., tactical allocations) from time-to-time adds value

MERCED COUNTY EMPLOYEES' RETIREMENT ASSOCIATION

RESOLUTION NO. 2024-01

Trustee Service Appreciation

Mr. David Ness

WHEREAS, Mr. David Ness was appointed to serve as a member of the Merced County Employees' Retirement Association Retirement Board and served as a member of the Retirement Board from July 2006, through February 2024; and

WHEREAS, Mr. David Ness participated in meetings by lending his expertise to the discussion of issues before the Retirement Board and made contributions to the Retirement Board by serving as the Board Chair for many years; and

WHEREAS, Mr. David Ness displayed commitment and worked for the interests of all members of the Retirement System throughout his tenure on the Retirement Board; and

NOW, THEREFORE, BE IT RESOLVED that the Retirement Board expresses its sincere appreciation for Mr. Ness's dedicated service to the members of Merced County Employee's Retirement Association and to the citizens of Merced County.

Ayes:

Noes:

Abstain:

Absent:

_____

Ryan Paskin, Chair

I hereby certify that on the 22nd day of February 2024, the Retirement Board of Merced County Employees' Retirement Association made and adopted this Resolution.

_____

Kristen Santos, Plan Administrator