Contents

CHIEF COMPLIANCE OFFICER LETTER

The Enterprise Compliance, Risk & Governance Office (ECRG) of the California Public Employees' Retirement System (CalPERS) coordinates, supports, and promotes an effective compliance and risk program throughout the enterprise. ECRG is at the forefront of compliance and ethics at CalPERS, working to protect the enterprise and its stakeholders by providing advice, guidance, and oversight which supports the enterprise's commitment to following all the laws, regulations, and policies that govern our organization.

The Annual Compliance Report outlines key accomplishments in compliance and risk activities covering the fiscal year (FY) 2023-24. Consistent with CalPERS' values of integrity, openness, and accountability, ECRG is keenly aware of our responsibility to set an example of ethical behavior and practices. We embrace partnerships with other program areas across the organization to leverage our effectiveness and maximize our impact. Our work relies on these relationships to help inform and raise awareness about the importance of compliance and ethics.

ECRG also recognizes that effective compliance and risk programs grow organically and that all team members understand their role in maintaining compliance and mitigating risks to CalPERS.

We hope this report demonstrates our commitment to compliance and the work we do to protect the system, the members, and the employer partners we serve.

Kevin L. Fein
Chief Compliance Officer

CULTURE OF COMPLIANCE

At CalPERS, we strive to embed compliance into the culture, strategy, and day-to-day business operations. All ECRG activities and accomplishments directly support our organization's strategic plan and core values.

During FY 2023-24, we continued to reinforce and expand upon advancing our strategic plan goal of organizational excellence by cultivating a culture of compliance, and a risk-intelligent organization. The program is in the process of several new multi-year initiatives that will continue to modernize the compliance, risk management, and governance program in the months and years ahead.

INTEGRATED ASSURANCE MODEL: THREE LINES OF DEFENSE

CalPERS embraces an Integrated Assurance Model to implement our compliance, risk, and governance practices and to promote a multi-faceted approach to compliance awareness and accountability. The model centers on a Three Lines of Defense framework (see Figure 1) emphasizing collaboration and an increased understanding of roles and responsibilities to detect, prevent, and correct instances of non-compliance.

Figure 1: Integrated Assurance Model
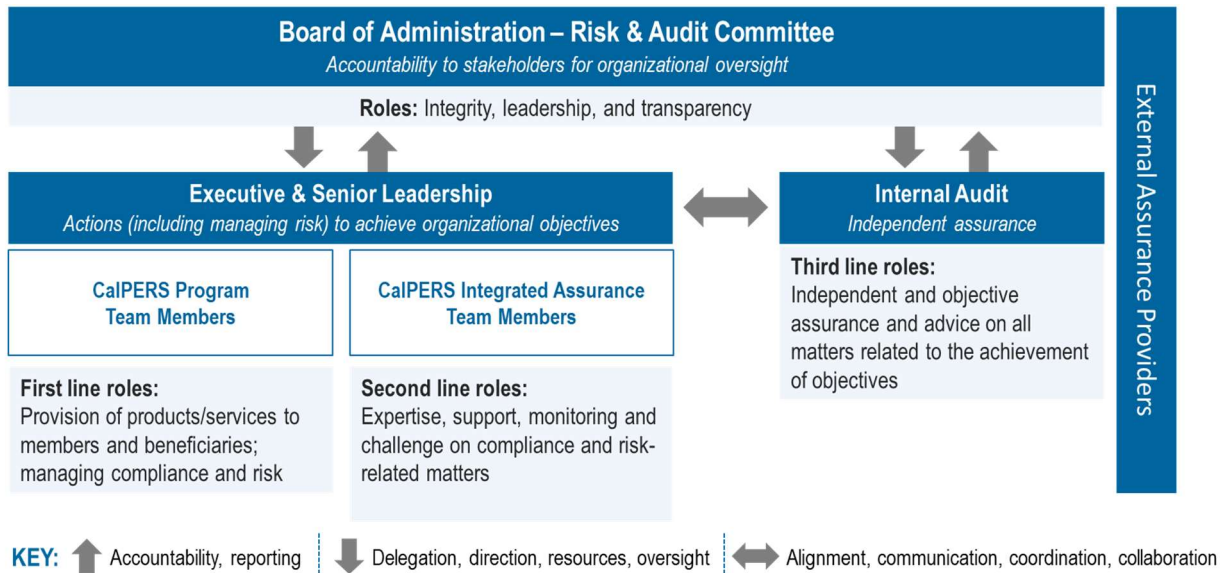
First Line of Defense – The first level of the control environment consists of the program areas that perform day-to-day risk management activities. As part of performing daily operations, the program areas are responsible for the design and implementation of internal controls to enhance compliance and

mitigate risks. They are closest to the program operations and have the best insight into actual or perceived risks and can have the opportunity to identify and prevent undesired outcomes.

Second Line of Defense – ECRG provides advice, guidance, and oversight of compliance, risk management, and governance activities. This structure provides increased capability to support the organization by mitigating strategic and operational risks while strengthening the organization's control environment and promoting strong ethical business practices and risk-informed decision-making.

Third Line of Defense – The CalPERS internal audit program provides independent assurance on the effectiveness of governance, risk management, and internal controls. The Office of Audit Services (OFAS) and ECRG participate in a joint, organization-wide risk discussion with leaders. This coordination helps CalPERS develop a shared view of risk across the organization.

The Integrated Assurance Model helps clarify roles and responsibilities and promotes ownership of compliance throughout the organization. Through the Three Lines of Defense, CalPERS encourages a "do the right thing" culture. By fostering a work environment based on our six core values, CalPERS recognizes that compliance is every team member's responsibility.

FY 2023-24 COMPLIANCE AND RISK INITIATIVES AND HIGHLIGHTS

ECRG has historically been guided by compliance standards set out in a variety of federal and state guidelines. The ECRG team, as well as partners from across the enterprise, significantly increase the sophistication, scale, scope, and quantitative analysis capabilities of the Compliance & Risk Program. The development goal will be to establish a best-in-class Enterprise Compliance Program consistent with private sector organizations operating similar functions of comparable size, scope, and complexity as CalPERS.

Conflict of Interest Oversight

ECRG led efforts across the enterprise to identify, manage, mitigate, and avoid conflict of interest with CalPERS employees, and organizations doing business with or the potential to do business with CalPERS. Conflict oversight includes but is not limited to attestation, monitoring, and disclosure of activities in areas such as personal financial-interests, personal trading, placement agents, vendor contracts, gifts, and travel. Rules and policies around conflict of interest are identified in CalPERS policies and government regulations.

ECRG launched the Gift and Entertainment Management Process within the MyComplianceOffice System. This involved onboarding all CalPERS team leaders and completing a phased rollout with live training sessions given to approximately 450 team leaders. The ECRG team also established a comprehensive information center and developed on-demand training modules to provide additional resources and guidance.

ECRG conducted approximately 200 compliance onboarding advisory sessions with prospective/new hires. These sessions educate and reinforce CalPERS compliance rules and a commitment to an ethical culture. New hires and their management are provided advice and guidance about the intersection of their role and financial interests with CalPERS conflict of interest rules.

ECRG administered the Placement Agent Regulation and reporting requirements to ensure compliance with the Regulation and disclosure of Placement Agent Fees, Gifts and Campaign Contributions from external managers seeking to do business with CalPERS.

All CalPERS Team Leaders participated in a review of their team member's 2022 Form 700 filings to aid in identifying potential conflict of interest based upon the team member's disclosures and their role at CalPERS.

The Operations and Technology Branch (OPT) facilitated 100% completion of the Annual Conflict of Interest and Confidentiality Certification & Disclosure Form that includes Board Members, Executives, and Senior Leadership.

Monitoring and Assurance

Monitoring and Assurance activities identify and measure material risk throughout the organization. Monitoring is focused on leveraging key metric reports to identify patterns, trends, and outliers in key processes that may indicate breakdowns and/or errors, requiring further investigation. Assurance Reviews are targeted scoped efforts to review key controls associated with requirements posing risk to the organization to ensure risk is being appropriately managed.

CalPERS achieved 100% compliance for the 2023 Annual Form 700 filing season and Annual Personal Trading Attestation period. The ECRG team conducted an enhanced review of 2022 Form 700 filings for all CalPERS Form 700 filers to ensure compliance with the FPPC rules and requirements.

ECRG, working with the various program areas, conducted intake on 140 new Ethic Helpline complaints, closed 121 complaints with thirty-eight substantiated. In addition, the overall handling time has improved with most complaints open an average of 120 days.

The Customer Services & Support (CSS) branch automated the disability retirement determinations and incorporated leader review and approval of all disability determinations in the myCalPERS system to ensure full compliance with relevant laws and regulations.

The Health Policy & Benefits Branch (HPBB) evaluated the Pharmacy Benefit Manager's clinical programs to assess compliance. They also completed Milliman quarterly HITRUST compliance checks and received updated Milliman background screening and HIPAA attestations.

ECRG collaborated with the Investment Office (INVO) to formalize the internal control and assurance review process, to ensure compliance with investment-related laws, rules, and regulatory requirements

that CalPERS is subject to. This team used a risk-based approach to focus and detail the controls of high impact investment program areas to conduct compliance assurance reviews.

ECRG developed and implemented enhanced performance and risk data points for various oversight and monitoring functions to create more meaningful reporting for senior leadership.

Advice and Education

Educate and cultivate ethical and risk-intelligent practices amongst CalPERS team members by providing advice and consultation on policy and regulatory requirements. Leverage training and educational programs to aid employees understand and comply with organization policies, standards, and regulatory requirements.

ECRG continued to cultivate a risk-intelligent and ethical culture by providing risk management, Form 700, and compliance training to new CalPERS team leaders and by conducting extensive compliance pre-hire and onboarding sessions to provide education and guidance to team members about compliance rules and disclosure requirements. The team enhanced tracking and reporting of the mandatory Attorney General's Ethics Training course in GoLearn.

The Actuarial Office (ACTO) improved employer education and communication to ensure appropriate financial management of agency pension plans. ACTO accomplished this by:

- Improving actuarial tools for modeling possible future pension outcomes and assessing financial management options available to our participating agencies.
- Improving actuarial valuation reports to allow for easier navigation and to provide other discussion/metrics regarding funded status.

HPBB completed their annual training assessment to ensure CalPERS users accessing MedInsight met CalPERS information security and HIPAA requirements.

The General Counsel Office (GCO) provided subject matter expertise to help monitor conflict of interests and Form 700 disclosure requirements. This included responding to inquiries on Form 700 filing requirements and conflict of interest issues under the Political Reform Act and related statutes and the development of related training.

OPT, in partnership with ECRG, streamlined the tracking and reporting of mandatory training compliance and reduced new-hire mandatory training times from thirty calendar days to fourteen calendar days to improve training compliance. OPT also facilitated the assignment of over ten unique mandatory training courses in GoLearn to more than 2,400 existing employees at the start of the fiscal year and over 270 new hires. Additionally, the mandatory training requirements for team members working in a training and development (T&D) assignment were updated by OPT, ensuring T&D participants would continue being assigned training required for their existing classification as well as their new role until the T&D assignment concludes.

Risk Assessment and Mitigation

Identify, assess, and manage risk within CalPERS to aid in ensuring compliance with regulatory requirements, CalPERS policies and standards, and industry best practices.

ECRG, in partnership with Information Technology Services Branch (ITSB), piloted the Risk and Controls Self-Assessment (RCSA) process with seven ITSB teams. In conjunction with the rollout of RCSA, OTP, also established an IT Technology Risk Committee to oversee, mitigate, and develop an IT technology risk report.

The RCSA process was also completed for the ECRG division. Additionally, ECRG collaborated with Investment Controls, and Operational Risk (ICOR) to enhance and refine the alignment of the investment-related laws, rules, and regulatory requirements to internal controls leveraging a risk-based approach.

ECRG also completed other key risk assessment and mitigation activities in partnership with program areas to include:

- 2023 Enterprise Annual Enterprise Risk Assessment partnering with key stakeholders across CalPERS.
- conducted reviews of high-rated audit observations to provide reasonable assurance that controls are still in place and operating as intended.
- successfully negotiated and renewed CalPERS Business Insurance Program policies working with GCO.
- partnered with the Office of Audit Services (OFAS) to conduct an annual enterprise-wide integrated risk assessment that supports the development of the annual audit plans.

CSS ensured consistency and risk reduction to the fund by discontinuing the Precautionary Retirement Application process and continuing to offer the emergency retirement process. CSS also enhanced its Online Notification Form to ensure compliance with the Use of Leave at Retirement Policy and mitigate unanticipated and unfunded liabilities for CalPERS. In collaboration with ITSB, they also strengthened the overpayment collection process to comply with state regulations.

INVO implemented information barriers to control the flow of material and non-public information.

OPT, in partnership with Colliers, ensured enterprise compliance with various State Fire Marshal audit findings to keep our buildings safe and up to code. OPT also developed and implemented a Disabled Veteran Business Enterprise (DVBE) tracker to ensure Contract Manager compliance with all DVBE contract requirements.

Data Privacy and Protection

CalPERS' ability to manage member and employee data collected lawfully and responsibly and protects the collected data from access or use by unauthorized parties.

ECRG participated in data management-related efforts with the Enterprise Data Management, Enterprise Data Council, and Data Steward Committee.

CSS digitized approximately eighteen file cabinets worth of data to protect sensitive information, mitigate the risk of fraud, and increase workload efficiency and transparency. In collaboration with the Public Affairs Office (PAOF), Information Security Office (ISOF), and ITSB, CSS also implemented technology solutions providing members with efficient and secure ways to access their warrant statements.

CSS's Customer Experience Division (CXD) and Customer Education & Outreach Division (CEOD) collaborated on several data privacy and protection initiatives. Together the two teams:

- Implemented upgraded authentication procedures to bolster security measures during phone and video interactions with customers.
- Revised authentication procedures specifically tailored for retirees, survivors, beneficiaries, and inactive members.
- Implemented a new front counter customer-side set-up with a customer-dedicated micro-PC and monitor with privacy screens at regional offices to protect sensitive information and improve information security practices.

HPBB updated the Privacy Notice Language to ensure CalPERS remains in compliance with the privacy policy in communication with members. HPBB also Identified newly developed and revised health data assets because of 2023 myCalPERS system enhancements, ensuring our data asset inventory in Archer is up to date and in alignment with the CalPERS Information Asset Classification Policy and Enterprise Data Management.

In addition, HPBB attended monthly Data Council meetings to discuss data retention, value, quantity, and security. Voting Data Steward and Enterprise Data Council members held positions on the Employer Data Request (EDR) Vetting Committee to review EDRs submitted by several business areas across the enterprise to ensure requests are thoroughly vetted before the release of CalPERS data. This extension of data governance supports the goal of ensuring EDRs are fulfilled accurately and efficiently and in compliance with laws and CalPERS security processes.

OPT reviewed enterprise software installations and followed through to promptly identify and remove any unauthorized software. In partnership with CSS, the Financial Office (FINO), and GCO, they also developed information asset retention periods to ensure appropriate retention of Terminated Member records.

Fraud Risk Management

Process of implementing measures, technologies, and strategies to prevent, detect, investigate, and mitigate fraudulent activities within an organization or across industries.

Fraud risk management continues to be a key enterprise priority. ERCG, ISOF, and GCO continue to partner to advance the program to include establish a new Fraud Governance body to monitor and mitigate fraud risk as well as enhance various fraud detection and fraud management processes.

Policy, Governance, and Reporting

Establishing CalPERS Policies, conducting governance routines for oversight and awareness at all levels of the management team and Board of Directors, and developing and delivering management reports internal and external as required to support risk processes.

ECRG completed the 2023 State Leadership Accountability Act (SLAA) Report Implementation Plan updates and submitted them to the Department of Finance. They also amended the CalPERS Conflict of Interest Code and onboarded 126 new filers. In addition, with the support of the GCO, ECRG continued to advance the compliance program enhancements.

FINO created new reserve policies for the CERBT and CEPPT funds and updated the SCP and 457 plan reserve policies. Additionally, they updated pension contracting forms to comply with federal accessibility guidelines.

HPBB strengthened the health plan compliance program through the recent PPO solicitation by increasing reporting requirements for the health plans in the areas of networks, quality, equity, behavioral health access, and telehealth. They also updated and revised data collection criteria in the automated system to improve Health Benefit Compliance and Appeals reporting for the CalPERS health branch stakeholders.

INVO updated the CalPERS Investment Policy for Insider Trading to include the allowance of Information Barriers within the Investment Office programs.

In partnership with CSS, FINO, and LEGO, OPT developed information asset retention periods to ensure appropriate retention of former health-dependent records. OPT also updated several policies and plans to ensure compliance with various requirements and standards. This included:

- Updating the Nepotism policy to comply with CalHR requirements.
- Revising the Excess Leave Reduction Policy, requiring team members to engage in leave reduction strategies, document those strategies in a Leave Reduction Plan, and adhere to the plan to bring their balances below the maximum number of leave hours allowed.
- Developing the Use of Leave at Retirement Policy following the state's mandated maximum number of hours allowed for paid leave including vacation, annual leave, voluntary personal leave, and compensating time off.
- Updating the Injury and Illness Prevention Plan.

- Regularly updating and modifying our COVID-19 Prevention Plan, per the Non-Emergency Temporary Standards.

Compliance and Regulatory Change Management

Identify and implement changes to business processes and practices to ensure compliance with changes in policies or regulations.

ACTO completed a comprehensive review of internal processes concerning HIPPA requirements and implemented process improvements to ensure continued HIPPA compliance.

FINO worked with the SIP program record keeper to comply with Secure 2.0 Act changes that were effective this fiscal year and updated the MYCP system to allow all employers to process Roth contributions to comply with future changes effective the next two fiscal years. They also updated the SIP Plan Document to include recent federal changes.

HPBB updated the supporting documentation requirements communicated as part of the Parent-Child Relationship (PCR) process, as well as disclaimer language displayed in myCalPERS and the PCR Affidavit and removed the dual signature and review requirement on the PCR Affidavit. Additionally, HPBB updated member communication and training and reference materials to align with the Social Security Administration's annual General Enrollment Period effective date changes and monitored federal and state health-related legislation impacting the CalPERS health program and policies to ensure regulatory compliance.

OPT refreshed the Records Retention Schedule to validate citations governing retention of each record type and classified each record as high, medium, or low consistent with the CalPERS Information Asset Classification Policy. OPT also transitioned the assignment of new leader appointment training to CalHR's Supervisor, Manager, and Executive Development Programs to meet Government Code 19995.4 mandates and the CalHR Leadership Training & Development Policy requirement. Additionally, they updated the CalPERS Leadership Training & Development Policy to comply and alignment with the CalHR Leadership Training & Development Policy.

SUMMARY

The Compliance and Risk program at CalPERS continues to mature and progress. The efforts of dedicated compliance and risk resources and our internal partners are a worthy investment in the long-term foundation of CalPERS' culture of ethical behavior and the processes that strengthen internal controls. Compliance and risk management elements are interwoven into all six of CalPERS' core values: quality, respect, accountability, integrity, openness, and balance. ECRG takes pride in leading these efforts and will continue to give guidance and direction as CalPERS strives to build a sustainable future based on a strong foundation of ethics, compliance, and risk management.