December 28, 2017

Marybel Batjer, Secretary
California Government Operations Agency
915 Capitol Mall, Suite 200
Sacramento, CA 95814

Dear Ms. Marybel Batjer,

In accordance with the State Leadership Accountability Act (SLAA), the Public Employees' Retirement System submits this report on the review of our internal control and monitoring systems for the biennial period ending December 31, 2017.

Should you have any questions please contact Forrest Grimes, Chief Risk Officer, at (916) 795-3616, Forrest.Grimes@calpers.ca.gov.

BACKGROUND

As the nation’s largest public pension fund, the California Public Employees’ Retirement System (CalPERS) manages pension benefits for more than 1.8 million California public employees, retirees, and their families. CalPERS’ membership is divided among current and retired employees of the State, schools, and participating public agencies. Additionally, CalPERS Health Benefits Program covers more than 1.4 million active and retired State, schools, and public agency employees and their families.

CalPERS was established by legislation in 1931 and became operational in 1932 for the purpose of providing secure retirement benefits to State employees. In 1939, new legislation allowed public agency and classified school employees to participate in the System. CalPERS began administering health benefits to State employees in 1962. Expansion in 1967 allowed public agencies to join the Health Program on a contract basis. CalPERS began offering longterm care insurance on a not-for-profit basis in 1995.

CalPERS is governed primarily by California Public Employees’ Retirement Law (PERL), Government Code Section 20000 et seq. CalPERS is administered by a 13-member Board of Administration (Board) who are elected, appointed, or hold office ex officio. Composition is mandated by law which can only be changed by a majority of the registered voters in the State. Constitutional and statutory laws give the Board exclusive control of the administration and investment of retirement fund assets, the authority to administer membership and benefit issues, and all powers reasonably necessary to carry out the health benefits program. The Board has the vested fiduciary duty to manage and control the following retirement systems, programs, and plans:

Public Employees' Retirement Fund
California Employers' Retiree Benefit Trust Fund
Judges' Retirement Fund
Judges' Retirement Fund II
Legislators' Retirement Fund
Public Employees' Deferred Compensation Fund
Public Employees’ Health Care Fund

Public Employees’ Long-Term Care Fund

Supplemental Contributions Fund

In addition to attending Board meetings, members may also serve on committees to review specific programs, projects, or issues and make recommendations to the full Board. The Board consists of six committees and a subcommittee:

- Board Governance Committee
- Finance & Administration Committee
- Global Governance Policy Ad Hoc Subcommittee
- Investment Committee
- Pension & Health Benefits Committee
- Performance, Compensation, & Talent Management
- Risk & Audit Committee

The Board also administers the Public Employees’ Medical and Hospital Care Act and the State’s contract with the federal government for Social Security.

CalPERS Vision & Mission

Vision - A respected partner, providing a sustainable retirement system and health care program for those who serve California.

Mission - Deliver retirement and health care benefits to members and their beneficiaries

Our core values of quality, respect, accountability, integrity, openness, and balance guide us in our work and interactions with our members, plan sponsors, and each other.

The CalPERS 2017-22 Strategic Plan focuses on the following five strategic goals:

- Fund Sustainability: Strengthen the long-term sustainability of the pension fund
- Health Care Affordability: Transform health care purchasing and delivery to achieve affordability
- Reduce Complexity: Reduce complexity across the enterprise
- Risk Management: Cultivate a risk-intelligent organization
- Talent Management: Promote a high-performing and diverse workforce

ONGOING MONITORING

As the head of Public Employees' Retirement System, Marcie Frost, Chief Executive Officer, is responsible for the overall establishment and maintenance of the internal control and monitoring systems.

Executive Monitoring Sponsor(s)

The executive monitoring sponsor responsibilities include facilitating and verifying that the Public Employees' Retirement System internal control monitoring practices are implemented and functioning as intended. The responsibilities as the executive monitoring sponsor(s) have been given to Charles Asubonten, Chief Financial Officer.
Monitoring Activities
Risk management is integral to achieving CalPERS’ Strategic Plan goal of cultivating a risk-intelligent organization. In support of this effort, CalPERS uses an integrated assurance three lines of defense model to implement and embed risk management and compliance responsibilities throughout the organization. Program areas are the first line of defense and internal control processes have been established to confirm that operations comply with laws, regulations, and policies to mitigate risks. Management across the enterprise continues to contribute to a risk management framework that includes consideration of risk in decision making, planning, and prioritization of business activities to achieve strategic and operational objectives.

The Enterprise Risk Management Division (ERMD) and the Enterprise Compliance Division (ECOM), are included in the second line of defense. ERMD is responsible for overseeing the enterprise risk management framework that includes the Enterprise Risk Management Dashboard, Risk Profiles, and Risk Heatmap. This team also facilitates risk management training, collects and analyzes emerging risk information, facilitates program risk assessments, and develops tools to assist the Board, executive team, and program areas in identifying, monitoring, and mitigating risks. ECOM is responsible for oversight of program area compliance with laws, regulations, and policies. This team designs, implements, tests, and monitors compliance processes within the program areas to evaluate the effectiveness of existing compliance strategies. ECOM also conducts compliance training and collaboratively promotes compliance throughout the enterprise.

The Office of Audit Services (OFAS) represents the third line of defense, by providing objective and independent validation through an independent reporting relationship to the Board. This team conducts assessments of the design and operating effectiveness of internal controls over business and technology operations, compliance with laws and policies, and effective management of risks.

The Board’s Risk and Audit Committee exercises oversight and monitoring of risk through periodic reports on the functioning of CalPERS’ risk management, compliance, and audit activities. Additionally, audits are performed by an independent financial statement auditor and other external auditors. Both management and the Board receive copies of all internal and external audit reports for review.

CalPERS' leadership groups are responsible for oversight of CalPERS' program area risks. Executive management meets formally monthly to review risk, compliance, and audit reports and findings, monitor performance and mitigation efforts, identify issues and concerns, and prioritize resources.

Addressing Vulnerabilities
CalPERS Audit Resolution Policy provides a system to track corrective actions or acceptance of risk taken by management on reported audit issues and to convey these actions to executive management and to the Board. Management has a responsibility to promptly evaluate reported audit findings, determine appropriate actions, and ensure resolution within an established time frame.

Quarterly status reports are provided to the Board and executive management on outstanding findings from Internal Audits, Public Agency Reviews, and External Audits. The Chief Auditor reports any risk acceptance to the Chief Risk Officer and executive management. The Chief Risk Officer tracks all accepted risks and includes these risks as part of the enterprise risk monitoring process as set out in the CalPERS Audit Resolution Policy.

Communication
CalPERS has several oversight leadership groups, including Information Technology Governance
Council, Integrated Assurance Risk Council, and Senior Leadership Council that meet regularly to
discuss issues, concerns, and foster improved communication across program areas. In addition,
CalPERS utilizes risk reporting tools that include the Risk Dashboard, Risk Profiles, and the Risk Heat
Map to track and communicate the status of the Enterprise Risks to the Board and executive
management. These documents are reviewed by the Risk and Audit Committee annually and shared
with all leadership and integrated assurance teams.

At the team level, select embedded liaisons are tasked to assist with the communication and
education of employees in the areas of risk and compliance. Additionally, the liaisons conduct ongoing
internal control monitoring, including the identification, resolution, and documentation of issues.

Ongoing Monitoring Compliance

The Public Employees' Retirement System has implemented and documented the ongoing monitoring
processes as outlined in the monitoring requirements of California Government Code sections 13400-13407.
These processes include reviews, evaluations, and improvements to the
Public Employees' Retirement System systems of controls and monitoring.

Risk Assessment Process

The following personnel were involved in the Public Employees' Retirement System risk assessment
process: Executive Management, Middle Management, Front Line Management, and Staff.

Risk Identification

CalPERS conducts an annual risk assessment with cross-functional teams and senior leaders across
the organization to review and update current and emerging enterprise risks. Results of the risk
assessment are documented in the Enterprise Risk Profiles and are provided to the Board semi-
annually. The profiles are comprised of the following components:

- Strategic alignment: each risk is defined by alignment to a strategic plan goal, the functional
  objective the organization is seeking to accomplish, and a risk statement that defines the
  consequence of the risk occurring.
- Risk analysis: a brief assessment of the inherent risk environment and evaluation of current
  control assurance to inform scoring.
- Risk score: the results of the scoring exercise.
- Risk drivers and mitigations: the identification of key factors that influence the ability of the
  organization to meet the functional objectives. For each risk driver, current mitigations and
  controls are documented, along with future mitigations that have been approved through the
  budgeting process.

Risk Ranking

Senior leaders and executive management score the risks in the areas of probability, impact, and
velocity on a five-point scale. Risk probability is defined as the likelihood that a given risk event will
occur; risk impact is the extent to which a risk event might affect the enterprise; and, risk velocity is the
speed of onset in which an organization feels the impact if a risk event occurs. In addition to these
three parameters, the scoring exercise includes the concept of materiality, which is the level of impact
at which a risk occurrence will threaten the achievement of a strategic or business objective, to help
establish common baselines for the risks. The scoring results are reflected in CalPERS Risk Heatmap
and in the finalized Risk Profiles, which are presented to the Board annually.
The top three risks to CalPERS are provided in this report. The full listing of enterprise risks can be found in the November 2017 Board item, Enterprise Risk Management Framework, reported to the Risk and Audit Committee on November 14, 2017 in agenda item 6.a. of the link below. [https://www.calpers.ca.gov/page/about/board/board-meetings/risk-201711](https://www.calpers.ca.gov/page/about/board/board-meetings/risk-201711)

---

**RISKS AND CONTROLS**

**RISK: OPERATIONS - EXTERNAL - TECHNOLOGY — DATA SECURITY**

*Functional Objective:* To ensure CalPERS’ information assets are safeguarded.

*Risk Statement:* Failure to protect and secure information assets.

The identified risk drivers are:

- Failure to adequately respond to a large-scale data breach and security incidents
- Lack of employee awareness of information security practices
- Inappropriate access to electronic information assets
- Inappropriate physical access to information assets
- Lack of compliance to policies and standards impacting information security

If this risk were to occur member privacy and the safety of CalPERS’ information assets may be compromised.

**CONTROL A**

*Annual Independent Security Assessments*

In an effort to test, improve, and validate the IT Cybersecurity Program, CalPERS annually hires third-party experts to perform independent security assessments. CalPERS uses the findings to strengthen the existing cybersecurity program by identifying opportunities for improvement, making necessary adjustments, and thereby reducing Information Security risk.

**CONTROL B**

*Information Security Policy*

CalPERS Information Security Policy specifies the rules that must be followed to protect CalPERS’ information, information systems, equipment, software, and people from a wide spectrum of threats and risks. All CalPERS’ employees and contractors annually acknowledge their responsibility in protecting CalPERS’ information assets and compliance with CalPERS Information Security Policies and Control Standards.

**CONTROL C**

*Information Security Control Standards*

CalPERS maintains an Information Security Control Library with up-to-date Information Security Control Standards that pertain to all employees, including third-party consultants and contractors, involved in conducting business for or on behalf of CalPERS. The Library also has a glossary, which includes terms related to information security.

**CONTROL D**

*Information Security Training*
Mandatory Information Security Training is completed annually by all CalPERS employees, third-party consultants, and contractors. This training reduces Information Security risk by equipping employees with the knowledge required to assess information security requirements, propose information security controls and ensure controls function effectively.

**Control E**  
**Information Security Monitoring and Detection**

CalPERS actively monitors information technology security activities and investigates security incidents in compliance with Information Security Policies and Control Standards.

**Control F**  
**Information Security Roadmap**

CalPERS is currently in the process of strengthening information security processes, system, and policies through an Information Security Roadmap Business Initiative. Through this initiative, CalPERS will establish a security governance program, enhance security policies, and perform necessary outreach and education to increase awareness, ensure adoption, and improve overall usability of the security governance program.

**Risk: Operations - External - Business Interruption, Safety Concerns**

Functional Objective: CalPERS' ability to resume business following a major business interruption.

Risk Statement: Inability to recover timely and resume business functions following a business interruption event.

The identified risk drivers are:

- Lack of agreed upon enterprise prioritization of critical and non-critical business functions
- Untested Division Business Continuity Plans
- Inability to restore critical business systems within expected timeframes
- System changes are not recorded and reported timely to the disaster recovery vendor
- Inability to react to an emergency
- Dependency on other State agencies to complete critical functions
- Mass regional disaster event impacting access to Emergency Operations Center

If this rise were to occur CalPERS' ability to carry out its mission may be interrupted.

**Control A**  
**Annual Review of Business Continuity Plan**

CalPERS implemented an updated Enterprise Business Continuity Plan to prioritize critical enterprise functions within the first 30 days following an event. Phase II of the Enterprise Business Continuity Plan, addresses full resumption of all enterprise business functions and operations.

**Control B**  
**Emergency Operations Center**

CalPERS maintains an off-site Emergency Operations Center (EOC) that can be activated in the event of an environmental, technological, or manmade hazard, or if a disaster disrupts CalPERS' ability to
conduct normal business operations. The EOC is monitored, and management routinely inventories supplies and tests functionality including bringing key systems on line. In addition, CalPERS regularly conducts business continuity exercises. This reduces Business Continuity risk by providing an alternate site to restore critical business systems within expected timeframes, and ensuring the EOC can support business resumption in the event of a disruption.

**CONTROL C**

**Disaster Recovery Exercises**

CalPERS conducts disaster recovery exercises to validate recovery plans and ensure restoration of critical business functions in the event of a major business interruption. This reduces Business Continuity risk by ensuring key leaders are ready to respond to an emergency and validating Division Business Continuity Plans.

**CONTROL D**

**Data Backup and Restore and Disaster Recovery Services**

CalPERS maintains a backup and recovery system at an alternate site to house critical business systems and data necessary for business resumption and alternative payroll processes with the State Controller’s Office.

**RISK: OPERATIONS -EXTERNAL-ECONOMIC VOLATILITY**

Functional Objective: To ensure the sustainability of the pension system to deliver retirement benefits.

Risk Statement: Failure to meet benefit obligations to current and future members and beneficiaries.

The identified risk drivers are:

- Financial markets suffer a severe downturn
- Investments fail to meet expected returns on an extended year-over-year basis
- Low funded status limits investment options
- Government constraints and regulations reduce portfolio diversification
- Employers default on contracted pension contribution payments
- Portfolio size and complexity challenges efficient investment processes and limits investment universe
- Actual experience deviates significantly from the actuarial assumptions
- Benefit design enhancements
- Employer contribution rate increases are insufficient to reduce unfunded liabilities over time
- Pension reform legislation or referendums that reduce employer obligation to honor pension contracts
- Judicial decisions that alter benefit design or contribution requirements
- Changes to actuarial standards

Market volatility, experience deviating from assumptions, and unanticipated legislation or referendums CalPERS’ mission to deliver pension and health care benefits to members and their beneficiaries may be compromised.

**CONTROL A**

**Funding Risk Mitigation Policy**
The Funding Risk Mitigation Policy seeks to reduce CalPERS funding risk over time. It establishes a mechanism whereby CalPERS’ investment performance that significantly outperforms the discount rate triggers downward adjustments to the discount rate, expected investment return, and correspondingly adjusts strategic asset allocation targets. The Policy aims to reduce the volatility of investment returns, thereby increasing the long-term sustainability of CalPERS pension benefits for members.

**CONTROL B**

**Stakeholder Education and Guidance**

CalPERS regularly communicates and engages with stakeholders to both seek and provide guidance, answer questions, and collaboratively resolve issues around pension liability. CalPERS hosts an annual Education Forum where employers can learn more about relevant issues, engage with CalPERS leadership, and schedule one-on-one consultations with the CalPERS team.

**CONTROL C**

**Asset Liability Management (ALM) Policy**

CalPERS Asset Liability Management Policy seeks to ensure contributions, plus investment returns, are sufficient to pay the benefits and expenses of the System. The ALM Policy provides a governance platform for implementing the Pension and Investment Beliefs, pursuing the key strategic goal of strengthening long-term pension fund sustainability, and carrying out the fiduciary duty owed to members. The strategic objective of the ALM Policy is to strengthen the long-term pension fund sustainability of the system. A key process supporting this objective is the ALM Review Cycle, which takes place every four years. This Policy establishes how employees oversee and coordinate the Four-Year ALM Review Cycle.

---

**CONCLUSION**

The Public Employees' Retirement System strives to reduce the risks inherent in our work and accepts the responsibility to continuously improve by addressing newly recognized risks and revising controls to prevent those risks from happening. I certify our internal control and monitoring systems are adequate to identify and address current and potential risks facing the organization.

**Marcie Frost, Chief Executive Officer**

CC: California Legislature [Senate (2), Assembly (1)]
California State Auditor
California State Library
California State Controller
Director of California Department of Finance
Secretary of California Government Operations Agency