CalPERS

Risk and Audit Committee
Agenda Item 4d

November 19, 2024

Item Name: Enterprise Risk Management Framework Review

Program: Enterprise Compliance, Risk and Governance

Item Type: Information Consent

Executive Summary

The purpose of this item is to update the Risk and Audit Committee on the current state of CalPERS' enterprise risks. The Compliance and Risk Oversight Team in Enterprise Compliance, Risk and Governance (ECRG) collectively worked with cross-functional workgroups comprised of subject matter experts, senior leaders, and the executive team to review and update all Enterprise Risk Profiles (Attachment 2). The organization's perception of enterprise risks is reflected and prioritized in the updated Enterprise Risk Dashboard (Attachment 1) and Enterprise Risk Heat Map (Attachment 3).

Strategic Plan

This agenda item supports the 2022-27 CalPERS Strategic Plan Goal – Operational Excellence: Cultivate a risk-intelligent and innovative culture through our team and processes.

Background

The Enterprise Risk Assessment began in September 2024 with the Compliance and Risk Oversight team conducted a series of assessments with cross-functional subject matter experts throughout the organization to review and update the Enterprise Risk Profiles. Risk drivers, high-level internal controls, and future mitigations were evaluated to reflect the current assessment of enterprise risks.

Enterprise risks are rated in the areas of probability, impact, and velocity. Probability is defined as the likelihood that a given risk event will occur. Impact is the extent to which a risk event might compromise the organization's ability to achieve its mission and strategic goals. Velocity is the speed of onset in which the organization experiences the impact if a risk event were to occur.

Analysis

The following enterprise risk reports were reviewed and updated:

- **2024-25 Enterprise Risk Dashboard** (Attachment 1) – provides the current rating of the top risks, risk categories, and risk statements identifying Board Committee and executive oversight.
- **2024-25 Enterprise Risk Profiles** (Attachment 2) – provides the Committee with detailed information on each enterprise risk. The Profiles are aligned to the CalPERS 2022-27 Strategic Plan and include the functional objective, risk statement and analysis, risk drivers and associated mitigation measures in place, and future mitigation measures, where applicable.
- **2024-25 Enterprise Risk Heat Map** (Attachment 3) – illustrates the probability and impact of the Enterprise Risks and the appropriate urgency of response.

Risk Profiles

The controls of each risk profile were updated or confirmed with no changes necessary to incorporate the organization's focus. The following is a summary of each risk profile.

Benefit Administration:

- To address team members' awareness of laws and regulations, an improved knowledge management system (myExpert) was implemented to provide quick access for informed decision-making. Improved death verification, notarization of benefit applications, and regular phishing exercises were implemented to improve fraud prevention controls. The resulting risk rating remains the same: High Impact/Low Probability.

Climate Change:

- The risk analysis to highlight climate solutions-related investments that help transition the economy to a low-carbon world was supported with enhanced controls. Plans for divestment from certain thermal coal companies based on SB185 that have an over-reliance on revenue from thermal coal mining were added as a control. The resulting risk rating remains the same: High Impact/High Probability.

Governance and Control Environment:

- No changes from last year's profile. The resulting risk rating remains the same: High Impact/High Probability.

Health Care Administration:

- To help ensure high-quality health care benefits, enhanced contract management, audits, and business review actions, a requirement for health plans to share demographic data with CalPERS was added as a control. The resulting risk rating remains the same: High Impact/Low Probability.

Information Security:

- The inability to identify and protect business systems risk driver was enhanced by adding a two-factor authentication control for remote access. The resulting risk rating remains the same: High Impact/High Probability.

Long-Term Care:

- To address increasing long-term care insurance premiums, an aging-in-place program was added as a control. The resulting risk rating remains the same: High Impact/High Probability.

Pension Funding:

- The shift from classic member formulas to an all-PEPRA population has been added as a control. The resulting risk rating remains the same: High Impact/High Probability.

Stakeholder Confidence:

- No changes from last year's profile. The resulting risk rating remains the same: High Impact/Low Probability.

Talent Management:

- Development of succession planning was added to the workforce plan as a control. The resulting risk rating remains the same: High Impact/High Probability.

Budget and Fiscal Impacts

Not Applicable

Attachments

Attachment 1 – 2024-25 Enterprise Risk Dashboard

Attachment 2 – 2024-25 Enterprise Risk Profiles

Attachment 3 – 2024-25 Enterprise Risk Heat Map

_____

Kevin Fein
Chief Compliance Officer