Risk & Audit Committee

California Public Employees' Retirement System

Information

Agenda Item 6a

November 17, 2015

ITEM NAME: Semi-Annual Enterprise Risk Management Plan, Update and Report (Dashboard)

PROGRAM: Enterprise Risk Management

ITEM TYPE: Information

EXECUTIVE SUMMARY

This agenda item provides a holistic view of the CalPERS risk environment through the Enterprise Risk Management Dashboard (Dashboard), which highlights 30 risk domains facing the organization and associated risk level and trends grouped into Strategic, Operational, Financial, and Compliance/Ethics categories.

A status update on key risk mitigation activities for the duration of May 2015 through October 2015 is included, as well as an overview of the four risk domains under the direct authority and oversight of the Risk and Audit Committee.

STRATEGIC PLAN

Enterprise risk management supports CalPERS 2012-2017 Strategic Plan Goal B: Cultivate a high-performing, risk-intelligent and innovative organization. To achieve this goal, 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.

BACKGROUND

Enterprise-wide risk assessments are periodically performed to identify, analyze, monitor, and mitigate risks. Results of these evaluations are presented on the Dashboard to the Risk and Audit Committee (Committee) on a semi-annual basis.

In October 2015, each Board of Administration Committee received an update on the risks related to its delegated duties. The agenda items sought to provide the committees with assurance risks are recognized, raised and managed

throughout day-to-day operations, while informing strategic and operational initiatives. Staff and committee members engaged in dialogue related to the challenges associated with the identified risks and resulting mitigation activities in progress.

These conversations provided the committees with an opportunity to confirm staffs' assessments and proposed rankings for the November Dashboard. Feedback included the need to highlight further the alignment of a committee's calendar, agenda items, and reporting with the management of its respective risk domains.

ANALYSIS

Risk and Audit Committee Risk Summary Report

The Committee's role, as outlined in Delegation No: RA-14-01, provides oversight and approval of the enterprise risk management framework, including the assessment and management of the entire landscape of risks. Additionally, the Committee has been identified as the most appropriate governing body for the direct oversight of the four risk domains within the Compliance/ Ethics category, as listed on Attachment 1.

Through daily activities and business initiatives throughout the organization, the four risk domains are being considered and addressed. The Risk and Audit Committee approved the established 2051-17 Enterprise Compliance Plan (Plan) in June 2015. The objectives of the Enterprise Compliance Plan are as follows:

- Promotes a culture of continuous improvement;
- Seeks to detect, correct and prevent potential instances of noncompliance; and,
- Achieves high ethical and compliance standards.

The Enterprise Compliance Plan identifies focus areas strategically designed to address Compliance & Ethics risks through initiatives such as:

- Leadership and Governance – Clarify leadership's roles, responsibilities and accountability in ensuring an ethical and compliant culture.
- Standards and Codes – Improve policy management tools, processes and governance.
- Operating Events and Incident Management – Establish policy and compliance incident management frameworks and reporting.
- Education and Communication – Enhance ethics and compliance education, training and communications.

Staff have focused resources and efforts on implementing new initiatives within the Compliance Plan which are designed to build new capabilities and address the Compliance / Ethics risks. As staff complete the initiatives, the risk levels and

trends are anticipated to decrease. Until that time, the risk levels will remain at Moderate and trending at Constant, to ensure continued focus and prioritization.

Progress on the Enterprise Compliance Plan is reported quarterly to the Risk and Audit Committee, and brief highlights related to the risk domains are below.

Ethical Conduct and Standards has remained at the Moderate-level and trending remains constant. Ongoing mitigation strategies include the CalPERS Ethics Helpline (Helpline) which provides confidential reporting to a third party. ECOM provides ongoing oversight and monitoring of the process, with quarterly reporting to the Risk and Audit Committee.

Additional mitigation strategies include the development of an initiative focused on compliance education, training, and communications. Enterprise Compliance staff are leading this effort, with recent progress made in the development of education related to key personnel changes, and enhanced training regarding Ethics Policies.

Fraud Detection and Prevention has remained at the Moderate-level and trending remains constant. In addition to the Helpline process, management has begun implementing mitigation strategies, including the development of an Operating Event management process, to identify, triage, and correct potential incidence of non-compliance discovered during “day to day” operations. ECOM staff developed training modules regarding the operating event process and have partnered with the Operations and Technology and Customer Services and Support branches to launch the process. This Operating Event process is already being used in the Investment Office.

ECOM staff have also partnered with Investment Office staff to enhance processes and policies to safeguard material nonpublic information, and ensure effective information barriers are in place.

Laws, Rules, and Regulations and **Policy and Procedures** have both remained at the Moderate-level and trending remains constant. Mitigation strategies related to both risk domains includes ECOM’s assumption of responsibility for the enterprise policy management and delegation of authority functions. ECOM has partnered with the Human Resources and Legal Office for input on the establishment of standards and frameworks for lifecycle management including processes, definitions, and oversight. Planned mitigation strategies include the creation of a policy and delegation of authority repository for ongoing management and maintenance.

CalPERS Risk Management Dashboard
The Dashboard (Attachment 2) provides a comprehensive view of the 30 risk identified for the organization, including risk description, committee assignment, and current risk level, and trends assigned through the recent assessment process. Table 1 further depicts the Dashboard risk levels and trends.

Table 1

Dashboard Risk Level	**Trend Upward**	**Trend Constant**	**Trend Downward**	***Risk Level Total***
Elevated	1	3	0	***4***
Moderate	11	3	4	***18***
Minimal	0	5	3	***8***
Trend Total	***12***	***11***	***7***	***30***

Included in the 30 risk domains, are three risks, stakeholder perception, legislative and regulatory, and governance/leadership which are not assigned to a Board committee and are detailed below.

Stakeholder Perception is one of the top five risks, and overall risk level has remained at a Moderate-level since October 2013. Risk trend level is now at a Downward trend given our successful outreach with stakeholders on risk mitigation, Environmental, Social and Governance (ESG) issues, and changes to our health care program. Staff does expect increased stakeholder outreach coordination in the foreseeable future as funding risks, renewed calls for pension reform, greater scrutiny over private equity fees and disclosure, and the upcoming health care excise tax are addressed. The activities below aim to help communicate the work being performed by CalPERS staff to respond to these issues and mitigate risks:

- CalPERS has expanded its outreach efforts to include a series of Employer Executive Visits with CalPERS executive leadership team to address top priorities and issues.
- Staff continue to hold regular stakeholder briefings, roundtables and individual meetings with key leaders of CalPERS member and employer associations.
- Staff is conducting the final phases of the Stakeholder Assessment Project, including a media analysis, in the coming months. The final results will be presented to the Committee in April 2016.
- Staff continue to develop messaging on key priorities and issues to ensure accurate and factual reporting in the media, including proactive steps to brief the media in advance where appropriate.

Legislative and Regulatory risk level will remain at Moderate-level with an Upward trend. Mitigation strategies include sustaining and supporting a proactive

legislative unit that provides education and outreach to members and staff of the Legislature on issues that impact CalPERS and our members. Going forward, Executive Liaisons will be expected to report to their respective committee on the risk level, challenges, and mitigation strategies specific to their responsibilities and delegated authorities.

Governance/ Leadership - Following discussion with CalPERS Executive Leadership within the Enterprise Risk Management Committee, this risk domain will be refined to provide better clarity. The risk level remains at Moderate-level with a Downward trend under the current definition, as below.

- Definition: The ability to collectively identify, understand and manage current and future risks effectively in a complex environment to support effective decision-making that guides CalPERS to meet its strategic goals and objectives.

CalPERS Risk Management Heat Map

Attachment 3 reflects the Risk Management Heat Map (Heat Map) which displays the 30 identified risk domains. The two factors used to determine the risk ranking levels, as shown in the matrix, are the likelihood of the risk to occur and impact of the occurrence for each risk domain. The Heat Map provides a relative ranking of each risk domain against other identified risks, along with an indication of where they fall within the red, yellow and green categorization spectrum. The higher the level of risk, the closer the domain is plotted to the red area of the heat map.

The top five risks, which have the greatest impact and high likelihood, are identified as:

- Pension Funding (Asset Liability Management)
- Business Continuity Management
- Participating Employer Financial Hardship / Insolvency
- Information Security
- Human Resources Management

These risks are carefully monitored within daily activities, subject of strategic and business initiatives, and are frequent topics of dialogue between staff and committees, such as with the:

- Board Workshop on Funding Risk and Mitigation - August 2015
- Review and discussion of the Funding Risk Mitigation Policy, Second Reading - October 2015
- Strategic Measure # 12 Findings: Employee Turnover - December 2015
- Quarterly Chief Information Officer IT Report - October 2015
- Annual Review of Funding levels and Risks Report - November 2015

Risk Management Heat Map Trends

Attachment 4 reflects the Risk Management Heat Map Trends (Heat Map Trends) and highlights the changes in the risk rating for the 30 identified risk domains since the last report in June 2015. The Heat Map Trends is organized by the change in risk level (increase, decrease or stable) since the last reporting period.

Of the 30 risk domains, two experienced an elevated change in risk level: Business Continuity Management and Information Security. The Finance and Administration Committee has oversight responsibility for both risks; a summary of each risk is provided below.

Business Continuity Management is one of the top five risks, and challenges associated with the potential for an unpredictable high-velocity event such as a cyber-threat or unpredictable major disruption to business operations. With an increased trend in data breaches, as well as environmental changes and natural disasters, or national security issues, staff have gained an increased awareness of the risks associated with today's environment. As a result, the risk domain was raised to an Elevated-level of risk with a projected trend of Constant.

Mitigation strategies include enterprise-wide integration and coordination of plans for business continuity, disaster recovery, and emergency response. Business Continuity Plans (BCPs) are developed and updated periodically to facilitate clear roles and responsibilities during times of an emergency, as well as identify interdependencies of key business processes and associated risks from disruptions by natural, technological, or human created hazards.

Information Security is one of the top five risks, and challenges associated with an expansion of sophisticated computer systems and software used to transact business activities is present with this risk. Constant evolution of the internet, applications, and systems expose critical information to possible misuse or theft; as a result, privacy and security rise to a high level of concern. As with business continuity, the increased trend in data breaches has provided staff with an increased awareness of the risks associated with today's environment. As a result, the risk domain was raised to an Elevated-level of risk with a projected trend of Constant, in recognition of CalPERS highly sensitive financial, health, and investment data and the every- evolving threat of cybersecurity.

2016 Risk Assessment

To further build a risk-intelligent organization that routinely focuses on strategic and operational risk management, the following are essential next steps in the 2016 Risk Assessment process:

- Integrated risk perspectives from Enterprise Risk, Enterprise Compliance, Audit, and Legal functions
- Refined risk categories that better align with industry terminology

    - Strategic: Created by, or affects business strategy decisions
    - Operational: Internal, preventable, and controllable
    - External: External forces that can affect ability to meet strategic objectives
- Refined risk definitions and mitigation strategies
- Refined methodology that enhances transparency and understanding of risk assessment methodology

As the risk landscape continues to evolve, staff will continue to seek the Committee's input on identified risks, ranking, and corresponding mitigation strategies to ensure the Committee can appropriately administer its delegated authorities.

BUDGET AND FISCAL IMPACTS
Funding for risk management activities is provided though the approved enterprise operating budget.

BENEFITS / RISKS
The Dashboard and Top Risk Report assist the Board to more effectively oversee enterprise risk management. The risk identification and recalibration process brings awareness to management to ensure that risk response strategies are in place to achieve business objectives and reduce risk.

Failure to monitor risks, trends, and mitigations may reduce the likelihood of attaining the benefits of effective enterprise risk management. Without regular reassessment and updates, risk information may fail to guide effective deployment of resources and significant risks may not be managed appropriately.

ATTACHMENTS
Attachment 1 – Risk and Audit Committee Risk Summary Report
Attachment 2 – CalPERS Risk Management Dashboard
Attachment 3 – CalPERS Risk Management Heat Map
Attachment 4 – CalPERS Risk Management Heat Map Trends

_____
CHERYL EASON
Chief Financial Officer