



## Agenda Item 6a

June 19, 2013

**ITEM NAME:** 2013-15 Risk Assessment Plan

**PROGRAM:** Office of Enterprise Risk Management

**ITEM TYPE:** Action

### **RECOMMENDATION**

Approve the proposed 2013-15 Risk Assessment Plan.

### **EXECUTIVE SUMMARY**

A primary component of CalPERS Risk Management Framework is conducting in-depth risk assessments to identify, analyze, evaluate, treat, communicate, and monitor risks on an on-going basis. An enterprise-wide risk assessment was conducted to identify current and emerging relevant risks that may impact the achievement of strategic goals and objectives. Based on the results, the Enterprise Risk Management Division (ERMD) prepared a Risk Assessment Plan for the Committee's review and recommendation to the Board of Administration. The proposed Risk Assessment Plan for Fiscal Year 2013-15 is Attachment 1 of this agenda item. This proposed Plan is designed to focus on CalPERS top risks and to provide assurance on management of the risks.

### **STRATEGIC PLAN**

This agenda item supports Strategic Plan Goal B: Cultivate a high-performing, risk-intelligent and innovative organization. A robust risk framework includes consideration of risk in decision making, planning, and prioritization of business activities.

### **BACKGROUND**

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."<sup>1</sup>

A robust risk assessment process forms the foundation for an effective enterprise risk management program. A risk assessment is intended to provide management with a view of events that could impact the achievement of goals and objectives. When assessments are performed systematically and consistently throughout CalPERS,

---

<sup>1</sup> Committee of Sponsoring Organizations, Enterprise Risk Management—Integrated Framework.

management is empowered to focus its attention on the most significant risks and make more informed risk decisions.

Risk assessment constitutes a key component of the Enterprise Risk Management Framework - risk identification. Conducting a risk assessment is a systematic process for identifying and evaluating events (i.e., possible risks and opportunities) that could affect the achievement of business objectives. Therefore, risk is defined as “the possibility that an event will occur and adversely affect the achievement of objectives.”<sup>2</sup>

An effective risk governance framework consists of three lines of defense. The three lines of defense model describes the alignment of the assurance providers in an organization and the interaction between the business management, other assurance functions, including Internal Audit. The role of ERMD, the second line of defense, includes:

- Providing the enterprise risk management framework.
- Collecting and analyzing risk information.
- Identifying known and emerging issues.
- Assists in guiding management to understand its risks and develop risk responses.
- Assisting management in developing processes and controls to manage risks and issues.
- Providing guidance and training on risk management process.

The individual risk assessments from all three lines of defense should be aligned (e.g., using common terminology, risk categories, and congruent outcomes), cover key business objectives, and be integrated to contribute to an enterprise-wide risk management program.

To develop the Plan, we considered the enterprise-wide risk assessment, CalPERS Enterprise Risk Dashboard, Top Risk List, the Information Security Risk Assessment Program, and internal audits as a foundation for developing this risk assessment plan as well as available ERMD resources. The Plan outlines the risk assessments that are on-going as well as new assessments to be performed during Fiscal Year 2013-14 and includes risk assessments in Fiscal Year 2014-15 anticipated to be performed. The plan will however be refreshed annually and adjusted according to the current risk environment.

The proposed Risk Assessment Plan was prepared to continue building CalPERS enterprise risk management program. The proposed risk assessments will provide an in-depth analysis of the risks domain. This includes developing a risk register outlining the inherent risk, controls, residual risk, and management’s risk response.

---

<sup>2</sup> Committee of Sponsoring Organizations, Enterprise Risk Management—Integrated Framework.

These risk registers will be continuously monitored and updated by management. ERMD will periodically assess the risk self-assessment, provide assurance on the assessment and treatment of the risk, and update the enterprise risk dashboard. Management, as the first line of defense, actively participates in the risk assessment process as described below:

- Identify and build the risk universe relevant to business objectives.
- Implement and maintain controls.
- Assess the likely and impact of risks.
- Develops risk responses and treatment plans.
- Monitors risks that may impact achievement of objectives.

### **ANALYSIS**

The principles of enterprise risk management require organizations to perform a risk assessment and implement a process to address and manage potential risks. By incorporating these requirements, we establish the following:

- Awareness through identification of risk.
- Planning through prioritization of risk.
- Development of risk responses and implementation of control mechanisms.
- Monitoring of risk and control activities.
- Assurances on management of risk.

The Enterprise Risk Management Division allocates 3.0 PY to the risk assessment activities outlined in the Plan.

### **BENEFITS/RISKS**

The risk assessment process, applied consistently throughout the organization, empowers management to better identify, evaluate, and manage the right risks, all while maintaining the appropriate controls to ensure effective and efficient operations and compliance with applicable laws, rules, and policies.

Without a cohesive, coordinated approach, limited risk and control resources may not be deployed effectively, and significant risks may not be identified or managed appropriately.

Approval of the proposed plan will focus the risk assessment efforts on CalPERS strategic issues and provide a basis for further development of the enterprise risk management program. Approval of the plan also advances CalPERS towards its strategic goal of becoming a risk intelligent organization. Failure to approve the plan may reduce the likelihood of achieving the strategic goal or advance the enterprise risk management program.

**ATTACHMENTS**

Attachment 1 – Proposed 2013-15 Risk Assessment Plan

---

LARRY JENSEN, Risk Officer  
Enterprise Risk Management Division

---

KATHLEEN K. WEBB  
Chief Officer of Risk, Compliance and Ethics

---

CHERYL EASON  
Chief Financial Officer