



Agenda Item 6c

August 14, 2012

ITEM NAME: Annual Risk Assessment Plan

PROGRAM: Enterprise

ITEM TYPE: Information

EXECUTIVE SUMMARY

The Risk and Audit Committee approved the attached Risk Assessment Plan for Fiscal Year 2012-13 (Attachment A) at the May 2012 meeting. The Risk Assessment Plan was subsequently updated to include the scope of each risk assessment in the plan as requested by the Committee.

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 currently and in the future. As one component of CalPERS Risk Management Framework, risk assessments are performed to identify, analyze, evaluate, treat, communicate, and monitor risks on an on-going basis.

The risk assessment results are reported to the Risk and Audit Committee on the Enterprise Risk Management Dashboard. The most significant risks are explicitly identified in the Top Risk Report which includes a summary of planned mitigation strategies. Management is responsible for managing and mitigating the risks identified through these risk assessments.

BACKGROUND

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
- Development of mitigation strategies and implementation of control mechanisms
- Monitoring of risk and control activities

“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.”¹

¹ Committee of Sponsoring Organizations, Enterprise Risk Management—Integrated Framework.

The proposed Risk Assessment Plan addresses strategic issues and aligns the risk assessment efforts to promote further development of the enterprise risk management program.

ANALYSIS

Risk assessment constitutes a key component of the Enterprise Risk Management Framework - risk identification. It is important to recognize the interrelationships between risk assessment and the other components of enterprise risk management (such as control activities and monitoring) and understand the principles and steps that help ensure the relevance and effectiveness of a risk assessment.

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, positively or negatively. Such events can be identified in the external environment (e.g., economic and political trends, regulatory landscape) and within CalPERS internal environment (e.g., people, process, and infrastructure). When these events intersect with CalPERS strategic or business plan objectives, or can be predicted to do so, they become risks. Risk is therefore defined as “the possibility that an event will occur and adversely affect the achievement of objectives.”²

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. Risk assessment methodologies may vary based on the type and level of assessment performed. Such assessments are used to assess strategic, operational, financial/reporting, legal/compliance, and reputational risk. There are various levels of risk assessment such as enterprise-wide, by division, business unit, and by processes. These risk assessments can be performed by division level staff and management, the Office of Enterprise Risk Management, or the Office of Audit Services.

To develop the FY 2012-13 Plan, we considered risk intelligence information gathered to date, as summarized within the current Enterprise Risk Management Dashboard and supplemental list of Top Risk. In addition, to integrate other risk assessments and assurance functions performed within CalPERS, we considered the results of prior information security risk assessments conducted by the Information Security Management Section, as well as prior audits and risk assessments conducted by the Office of Audit Services. Based on the information gathered, and after considering outcomes from CalPERS’ strategic planning meeting conducted in April 2012, the risk management plan was aligned with CalPERS strategic direction. In collaboration with the Office of Audit Services the risk assessment and audit plans were coordinated to assess the extent of coverage and whether a risk assessment or audit should be conducted.

² Committee of Sponsoring Organizations, Enterprise Risk Management—Integrated Framework.

The Risk Assessment Plan was prepared to continue building CalPERS enterprise risk management program. It integrates various types of risk assessments, including strategic, operational, information security and privacy, and compliance.

BENEFITS/RISKS

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.

ATTACHMENT

Attachment 1 – Risk Management Plan for Fiscal Year 2012-13.

LARRY JENSEN, Risk Officer
Enterprise Risk Management Division

Kathleen K. Webb
Chief Officer of Risk, Compliance and Ethics
Office of Enterprise Risk Management

RUSSELL G. FONG
Acting Chief Financial Officer