Risk & Audit Committee

California Public Employees' Retirement System

Agenda Item 5a

May 15, 2012

ITEM NAME: Annual Risk Assessment Plan

PROGRAM: Enterprise

ITEM TYPE: Action

RECOMMENDATION
Approve the proposed Risk Assessment Plan for Fiscal Year 2012-13.

EXECUTIVE SUMMARY
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. When assessments are performed systematically and consistently throughout CalPERS, management is empowered to focus its attention on the most significant risks and make more informed risk decisions.

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 Office of Enterprise Risk Management prepared an Annual Risk Assessment Plan for the Committee's review and recommendation to the Board of Administration. The proposed Annual Risk Assessment Plan for Fiscal Year 2012-13 is Attachment 1 of this agenda item.

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.

An effective risk governance framework consists of three lines of defense.

- The CalPERS divisions are closest to risk in day-to-day operations and are the first line of defense. Understanding and managing risk is embedded or woven in to management's everyday job to achieve their performance objectives.
- The Office of Enterprise Risk Management (OERM), the second line of defense, (1) establishes the enterprise risk management framework, (2) assists in guiding management to understand its risks and develop risk responses. The enterprise risk management framework is an on-going process of continuous risk identification, monitoring, evaluation, and treatment of risk and is forward-looking. Through this process, OERM facilitates and assists in normalizing risk across the enterprise to help management and the Board with a systematic approach to understanding risks to make informed decisions.

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

- Risk assessment is also a necessary component of an effective internal audit program. The Office of Audit Services, as the third line of defense, performs an annual risk assessment for the purpose of developing its annual audit plan, as required by professional standards.

The following table illustrates differences between risk assessments performed as part of an Enterprise Risk Management (ERM) program and internal audits:

ERM Risk Assessment	**Internal Audit**
Assist in guiding management in understand its risk and develop risk responses and mitigation plans, and aid management and the Board in enterprise decision-making.	Provide independent and objective assurance to the Board and management regarding internal controls or other audit objectives.
Provides facilitated management self-assessment and risk management plans. Prepares reports to management and the Board to understand risk exposures and response plans.	Conducts testing of evidence and draws conclusions, develops recommendations to management, and communicates findings through audit reports.
May conduct independent assessment. Best Practices.	Independent assessment. Established principle and standard.
Train and coach management to help them become more aware of risks in their everyday work.	Conveys recommended best practices but does not engage in training management.
Assist management with development of policies and procedures, and internal controls.	Recommends business practices, but must not prescribe policy or procedures or internal controls.
Able to provide reasonable assurance to management and board that risk responses are adequate and achieving intended outcome.	Provides independent assurance to the Board that internal controls are effective and managed properly.
Flexible in approach for conducting risk assessments and reports; follows best practices and business judgment.	Follows formal professional standards in conducting audits, reporting, and follow-up on prior recommendations.
Integral part of the internal control structure and performance management.	Evaluates the internal control structure.
Intended to provide management with a view of current and future events that could impact the achievement of goals and objectives.	Audit plan to set the direction and priorities of the specific internal audit activities and allocation of audit resources.
On-going and continuous risk assessment flowing through an entity.	Periodic project for risk assessment and audit.

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.

The proposed 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. We considered the CalPERS Enterprise Risk Dashboard, Top Risk List, the Information Security Risk Assessment Program, and internal audit risk assessments as a foundation for developing the risk assessment plan as well as available ERMD resources.

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. Failure to approve the plan may reduce the likelihood of advancing the enterprise risk management program.

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

LARRY JENSEN, Risk Officer
Enterprise Risk Management Division

RUSSELL G. FONG
Acting Chief Financial Officer