# Consent

## Agenda Item 4e

September 16, 2014

**ITEM NAME:** Quarterly and Year End Status Report – Enterprise Risk Management

**PROGRAM:** Risk Management

**ITEM TYPE:** Information Consent

**EXECUTIVE SUMMARY**

This reporting item provides a current status update of key activities and accomplishments of the Enterprise Risk Management Division (ERMD), from April 1 through June 30, 2014.

**STRATEGIC PLAN**

This agenda item supports CalPERS 2012-2017 Strategic Plan Goal B: Cultivate a high-performing, risk-intelligent and innovative organization. ERMD is actively participating in development and implementation of the following 2013-15 Business Plan initiatives:

- Policy Management – Develop a Policy Management framework to establish an enterprise-wide policy oversight approach and compliance function.
- Information Security Roadmap – Implement Information Security Roadmap to enhance security measures designed to protect information assets.
- Strategic Risk Measures – Create risk appetite statements, tolerances, and key risk indicators for strategic goals and top risks of the organization.

**BACKGROUND**

An effective enterprise-wide risk management program provides a holistic approach to the identification of organizational risks, risk responses, internal control activities, and continuous risk monitoring. ERMD serves as a trusted advisor to CalPERS and its business partners on enterprise-wide risks, information security, privacy, HIPAA, business continuity and policy development. ERMD also creates and administers information security, privacy and HIPAA policies; conducts and reports on enterprise-wide risk assessments; administers the enterprise policy framework; provides awareness training (risk, privacy, information security, and business continuity); and facilitates business continuity planning and response.

**ANALYSIS**

The following were accomplished during this reporting period to further mature the risk management processes while providing executive management and the Board reasonable assurances that key risks are being identified and mitigated.

Annual Risk Assessment Plan

During the quarter, ERMD continued to perform risk assessments outlined in the Fiscal Year 2013-14 Annual Risk Assessment Plan which included the following:

- Completed a cloud computing services risk assessment. The results of the cloud computing risk assessment will serve to guide CalPERS in addressing the new challenges and risks to the organization and the development of governance and control processes for cloud computing services, which is expected to increase in the future.
- Upon request by the Legal Office, initiated a fiduciary insurance coverage risk assessment. The objective of this risk assessment is to determine whether our treatment of the risks via fiduciary insurance is appropriate or whether we need to explore possible changes.

In addition, ERMD completed an enterprise risk dashboard recalibration to provide an overview of CalPERS risk environment. Based upon the results, the top ten risk domains were identified and represent the areas of risk that have the most significant impact and likelihood of affecting the achievement of our strategic goals and objectives. Overall, the level of risk intelligence continues to advance across the organization with an increased level of participation by the Division Chief Council in the completion of the risk registers supporting the enterprise risk dashboard. The Enterprise Risk Management Dashboard and the Top Risk Report were presented to the Enterprise Risk Management Committee and the Risk & Audit Committee at the June meetings.

Business Continuity Management

In response to the request by the California Office of Emergency Services (CalOES), ERMD reviewed our Administrative Order to ensure compliance with Governor's Executive Order W-9-91 and for consideration of additional response activities requested by CalOES. In addition to our requirements for ensuring emergency planning, preparation, training and participation during a proclaimed disaster or emergency, we have also added the provisioning of specialized and trained staff to assist CalOES in an emergency situation (i.e. translation services).

ERMD continues to ensure CalPERS readiness to respond to a disruption by maintaining oversight and managing availability of business continuity resources and tools at the Emergency Operations Center (EOC). With the recent expansion to the West Sacramento facility, ERMD initiated planning and preparations with consultant, Borden Lee Consulting, to create an evacuation plan for that facility.

Additional readiness activity included: emergency supply inventory and replenishment for the Lincoln Plaza buildings and the EOC; the distribution and activation of business continuity plan documents on new USB devices for all Executive Staff; conducting Emergency Operations Center (EOC) tour for Executive Staff; ongoing assessment of business requirements to effectively automate the

business continuity process in the RSA Archer eGRC Solutions platform designed to enhance planning and response.

Enterprise Governance, Risk and Compliance (eGRC)
ERMD continues to move forward with development and implementation of the RSA Archer eGRC solutions platform that will significantly enhance our ability to identity, assess and monitor risks across the enterprise. ERMD staff and project managers are engaged and assigned roles and responsibilities to ensure the Archer modules are implemented within the planned timeframes (schedule) and budgeted resources (costs), and meet requirements/expectations for functionality (scope). Phase 1 of the Archer Strategy/Roadmap has been implemented and includes Investment Office Operating Events, Enterprise Risk Assessment, Risk Register Recalibration, and the Compliance Review Process. Phase 2 projects are in progress and include Business Continuity Management/Disaster Recovery, Incident/Case Management and the HPAD Appeals Process.

Information Security Roadmap Program
ERMD provided direction, oversight, and served as a trusted advisor to the Information Security Roadmap Program (SRP) FY13/14 projects. CalPERS business requirements, laws/regulations, and best practices were analyzed to create new Information Security Policies and Control Standards, which govern the enhanced information security capabilities the SRP projects deliver.

ERMD defined the information asset classification specifications within the eGRC platform for the SRP Data Loss Prevention project. This enables the new tool to more effectively assist CalPERS business areas to correctly identify, classify, and protect their information assets.

Policy Management
To implement the 2013-15 Business Plan initiative for Policy Management, ERMD has refined the policy and procedures management framework. This framework delineates a policy “life-cycle” governance process that defines how a policy is created, maintained and retired. The framework includes policy, tools, templates, and a proposed governance process for the management of enterprise policies and procedures. Activities included:

- In response to a major update to the US National Institute of Standards and Technology (NIST) Security and Privacy Controls, ERMD updated the CalPERS Information Security Control Standards. This maintains a close alignment of the CalPERS information security program with US Government information security and privacy standards.

- ERMD incorporated the Information Security Control Standards into the CalPERS Enterprise Content Management system (SharePoint) and retired the prior ERMD

Information Security Principles, Policies, and Practices that have been governing CalPERS information security activities for over a decade.

- ERMD created additional Information Security Control Standards for "Cloud Computing". Together with policies from other CalPERS areas, these will serve to govern and establish the appropriate internal controls for this new growing technology service.

Privacy and Information Security Oversight

The first phase of the transformation of the HIPAA Privacy program into an Enterprise Privacy Program has been completed. This provides a foundation for the subsequent expansion and maturation of privacy related activities to ensure we are broadly assessing and monitoring to protect the privacy of our members, stakeholders, and employees information in a dynamic information security environment.

As part of its information security oversight responsibilities, ERMD has planned an extensive analysis of the current CalPERS information security defensive measures and capabilities. This analysis has been significantly expanded from previous analyses and will evaluate a wider range of information security factors. It will be performed independently by a nationally recognized company which specializes in this type of analysis. The results of this analysis will guide our ongoing risk assessments to ensure we are prioritizing activity to address changes in the security environment.

Strategic Risk Measures

ERMD developed a Strategic Risk Measures KRI Model roadmap and project plan for the development of key risk indicators linked to strategic measures and top risks for implementation in the FY 14-15 project cycle. To ensure a coordinated approach, ERMD will continue to collaborate with ESPD in the development and alignment of key performance measures with key risk indicators that directly contributes to the cultivation of a high-performing, risk-intelligent and innovative organization.

**BENEFITS / RISKS**

The achievement of the CalPERS 2012-2017 Strategic Plan Goal B: Cultivate a high-performing, risk-intelligent and innovative organization provides significant benefits to the organization:

- Effective information security and privacy practices provide assurance to CalPERS members and business partners that their information is safe with CalPERS.
- Incorporating information security controls into business systems and processes enables CalPERS to safely provide new and enhanced online services.
- Improved governance of the organization through establishment of an enterprise policy lifecycle management framework.

- Policies protect the organization by defining, articulating and communicating boundaries and expectations.
- Key risk indicators provide an early signal of increasing risk exposures that may adversely impact achievement of the strategic goals and objectives.
- Risk assessments inform management if mitigation strategies need to be employed to reduce the level of risk. This will improve risk-informed decision making.
- Business Continuity Planning is essential to resume CalPERS mission critical services to our members in the event of a disaster.

Implementing the activities outlined in this agenda reduces CalPERS to the exposure to the following risks:

- Financial risks due to consequences of failure to protect member information (i.e., litigation, credit protection, etc.).
- Reputational risks resulting from large and/or on-going breaches of sensitive data.
- Reduces risk in the confidentiality, integrity, and availability of our systems.
- Achievement of strategic goals and business plan objectives.
- Ability to provide member services after a disaster.
- Compliance with policies.

**BUDGET AND FISCAL IMPACTS**
Resources for the initiatives outlined in this ERMD status report are funded by existing internal resources. No additional funds are being requested at this time.

**ATTACHMENTS**
N/A

_____
KATHLEEN K. WEBB
Chief Risk and Compliance Officer

_____
CHERYL EASON
Chief Financial Officer