Consent

Agenda Item 5d

March 17, 2014

ITEM NAME: Enterprise Risk Management Division Status Report

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), as of February 16, 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:

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

BACKGROUND

ERMD conducts and reports on enterprise-wide risk assessments, oversees and administers the policy governance framework, has oversight of privacy and information security policies, provides awareness training (risk, privacy, security, and business continuity), and facilitates the business continuity program. An effective enterprise-wide risk management program provides a holistic approach to the identification of organizational risks, creates an appropriate risk response, develops internal control activities, and continuously monitors and reviews the risks. The CalPERS Board of Administration (Board) approved a Fiscal Year (FY) 2013-14 Annual Risk Assessment Plan that outlines the specific risk assessments to be performed.

ANALYSIS

The following topics were addressed 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.

Information Security Roadmap

The Information Security Management Section (ISMS) provides oversight and serves as a trusted advisor in the development and implementation of the Information Security Roadmap Program (SRP) projects. To support implementation of these projects, ISMS created new Security Policies and Control Standards to ensure the projects conform to current CalPERS Information Security Policies and industry best practices for the safeguarding of CalPERS information assets. In addition, ISMS continuously monitors implementation of the SRP projects to assess the impact upon information security risks to the organization.

Policy Management

To implement 2013-15 Business Plan initiative for Policy Management, ERMD has created a new 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 a policy, tools, templates, and a proposed governance process for the management of enterprise policies and procedures.

A communication plan and training plan have been developed to promote awareness of the new policy and procedures framework and ensure continuity for successful transition to this centralized enterprise policy model. These plans will be fully implemented by June 2014, consistent with the Business Plan.

Strategic Risk Measures

ERMD focused on best practices for developing key risk indicators. We conducted research into how organizations are designing, monitoring, and reporting key risk indicators (KRIs) to improve risk-informed decisions. KRIs can be designed to alert management to trends that may adversely affect the achievement of the Strategic Plan Goals and Objectives. ERMD continues to coordinate with ESPD to connect the strategic risk measures to the KRIs.

Annual Risk Assessment Plan

The Enterprise Risk Assessment Section (ERAS) is performing the risk assessments as outlined in the FY 2013-14 Annual Risk Assessment Plan. Specifically, ERAS conducted a risk assessment to assess compliance with CalPERS information security policies and standards for the Investment Office and the Enterprise Compliance Division.

ERAS also initiated a risk assessment of Cloud Computing Services in response to an audit finding on this topic. ERAS identified the risks associated with the use of Cloud Computing Services and selected four Services used at CalPERS to assess the degree of exposure. In addition to the risk assessment, ERAS is participating in a workgroup to develop and recommend an appropriate cloud computing strategy and governance policy. ISMS developed information security Policy/Control Standards for CalPERS based on industry best practices and is implementing oversight capabilities to monitor for compliance with the Standards.

Privacy and Information Security Oversight

The CalPERS Privacy Program is being enhanced to fully meet the requirements of Government Code and State Policy (SAM 5300) for assessing compliance to secure confidential and sensitive information assets.

HIPAA governance was incorporated into the PeopleSoft contract approval processes to ensure Business Associate Agreements are included, as necessary, for technology services.

A new Security Policy for my|CalPERS was developed and implemented in the first my|CalPERS Identity Access Management (CalIAM) system implementation. The objective is to ensure that access to data is appropriately established to safeguard our information assets on behalf of our members.

Business Continuity Management

The Emergency Management (EMAN) section conducted several tours of CalPERS' Emergency Operations Center (EOC) for the Executive Team, Division Chiefs, Emergency Operations Team, and the California Office of Technology to become familiar with the facilities.

Training was conducted with the Executive Team and the Emergency Operations Team on implementing the Incident Command Structure at the EOC. The training reviewed EOC roles and responsibilities along with crisis management techniques to respond to an emergency and provide for business resumption and continuity to serve our members.

EMAN also completed an analysis of CalPERS business continuity plans to verify compliance with Cal Office of Emergency Services standards. EMAN continues to work with the Division Chief Council and ITSB to ensure consistency between business continuity planning and the technical Information Technology recovery plans. The Business Continuity Plans are critical to ensure that we can immediately assess, prioritize and initiate business resumption activities following a major incident.

The Executive Risk Management Committee reviewed the Offsite Exercise After Action Findings and Recommendation Report. The exercise allowed us to identify areas to enhance our response and include the identification of additional evacuation sites and the development of an Emergency Management Toolkit as a “grab and go” tool to assist management in the event of a real evacuation.

Projects
eGRC Platform **-** To improve efficiency, an Enterprise Governance Risk and Compliance (eGRC) solution is being implemented to automate certain functions for risk management, compliance, event management, business continuity, and policy management. The event management function was implemented for the Investment Office (INVO) to track and report risk and compliance events. Thus, allowing INVO to track management of these events and reduce risk of loss or lack of compliance with investment policy. The system was also configured to automate the enterprise-wide risk assessment, recalibration of the risk dashboard, and compliance assessments.

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:

- Robust information security measures to safeguard CalPERS systems and data. Oversight of information security and privacy also provide assurance that CalPERS complies with applicable laws, regulations, and policies.
- 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 and data.
- 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.

LARRY JENSEN, Chief Risk Officer
Enterprise Risk Management Division

KATHLEEN K. WEBB
Chief Risk and Compliance Officer

CHERYL EASON
Chief Financial Officer