Consent

Agenda Item 4e

November 18, 2014

ITEM NAME: Quarterly 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 July 1 through September 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 the development and implementation of the following 2014-16 Business Plan initiatives:

- Information Security Roadmap – Implement risk mitigation strategies to enhance management of security events, access to information and data loss prevention to safeguard information assets.
- Strategic Risk Measures – Create a direct link between the organization's strategic measures and the enterprise top risks using key risk indicators to enhance risk-informed decision making and achievement of strategic goals.

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 in the management of 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 actions 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 make progress on the risk assessments outlined in the Fiscal Year (FY) 2014-15 Annual Risk Assessment Plan. An overview of the CalPERS insurance program was presented to the Enterprise Risk Management Committee (ERMC) in August, which included the following recommendations:

- CalPERS to obtain an independent insurance assessment to identify gaps and present recommendations for addressing and mitigating insurable risks.
- Pursuant to the assessment, evaluate current rules and policies to ensure alignment with Public Employees Retirement Law accounting requirements.
- Conduct annual insurance assessments and coordinate this activity with the Investment Office real estate insurance review.

In addition, ERMD initiated an enterprise risk dashboard recalibration to provide an updated overview of CalPERS risk environment. During the recalibration process, all the risks were reconsidered in terms of impact and likelihood of affecting the achievement of our strategic goals and objectives. This activity also included aligning the risk domains on the Enterprise Risk Management Dashboard to respective Board Committees which supports the delegated responsibilities and further embeds risk-based decision making in our processes.

Business Continuity Management

ERMD continues to ensure CalPERS readiness to respond to a disruption by maintaining oversight and managing availability of business continuity resources. ERMD recruited and updated the Floor Warden and Emergency Response Team to fill vacancies resulting from the division moves throughout Lincoln Plaza and the West Sacramento location. ERMD planned and facilitated an Emergency Response and Floor Warden Team training with consultant, Borden Lee Consulting, to ensure preparedness for emergency response. ERMD also finalized planning and preparations with the consultant to create and distribute an evacuation plan for the West Sacramento facility.

Additional readiness activities included: creating a manager toolkit to assist in evacuation drills, ongoing assessment of business requirements to effectively automate the business continuity process in the RSA Archer eGRC platform designed to enhance planning and response, and initiating preparation for CalPERS participation in the California Great Shake Out.

Enterprise Governance, Risk and Compliance

To improve efficiency, an Enterprise Governance Risk and Compliance (eGRC) initiative has been implemented to automate certain risk management, compliance, incident management, business continuity, and policy management functions. During this reporting period, we rolled out two solutions as part of the second phase of the eGRC Project, which included (1) the Business Continuity Management solution, which will allow the integration and centralized management and testing of business

continuity and disaster recovery plans, and (2) the Incident Management solution, which will automate the work flow processes for improved oversight and handling of sensitive and/or classified incidents.

Information Security Roadmap

ERMD provides direction, oversight, and serves as a trusted advisor to the Information Security Roadmap Program (SRP) FY 14-15 projects. CalPERS' business requirements, laws/regulations, and best practices are analyzed to create new Information Security Control Standards, which govern the enhanced information security capabilities the SRP projects deliver. ERMD uses these Control Standards to guide the development and implementation of the SRP projects. The Information Security Policies and Control Standards are also used as a basis for planning the budget requests that are currently under development for the future SRP FY 15-16 projects.

ERMD created business processes to protect data identified by the new Data Loss Prevention (DLP) capabilities implemented in the SRP FY 14-15 DLP project. These business processes will help CalPERS business areas to correctly classify and protect their information assets.

In conjunction with the SRP FY 14-15 Enterprise Identity System (EIS) project, ERMD has created business processes and specifying the business rules that identify suspicious activities within the myICalPERS system with an established response process when these activities are detected. These enhancements will serve to strengthen our fraud management capabilities within the myICalPERS identity management system to protect the information assets of our members and employers.

ERMD has specified 34 Information Security Control Standards and developed 61 functional requirements for the SRP FY 14-15 Security Information and Event Management (SIEM) project. This project will enhance CalPERS ability to detect security issues and perform forensics examinations. ERMD also continues to act as a major stakeholder and trusted advisor to the SRP FY 14-15 SIEM project.

Policy Management

ERMD has refined the policy and procedures management framework to delineate within the policy "life-cycle" the process that governs policy creation, maintenance and retirement. The framework includes policy tools, templates, and a proposed governance process for the management of enterprise policies and procedures. Additional activities included:

- Implementing a phased approach to converting policies into the new standardized templates that support the governance process and life-cycle management.

- Utilizing the California State Administrative Manual (SAM) as the guiding authoritative source for statewide policies, procedures, and requirements, ERMD has incorporated SAM Section 5300, which governs information security, into the CalPERS information security policy framework and created new Control Standards to support the policies.

- Utilizing the California Statewide Information Management Manual (SIMM) standards required by state agencies to comply with the Information Technology policy, ERMD has incorporated the SIMM sections into the CalPERS information security policy framework and created new Control Standards to support them.

- Development of the new CalPERS Cloud Services Policy which will govern CalPERS use of "Cloud Computing" utilizing the previously developed Information Security Control Standards as a guide.

Privacy and Information Security Oversight

ERMD is in the second phase of maturing the HIPAA Privacy program towards an enterprise privacy program that effectively manages the specific risks while integrating oversight responsibilities and processes for program efficiencies. This effort mirrors industry best practices and the resulting privacy program will provide a foundation that will increase our capabilities to assess and monitor CalPERS activities that protect the privacy of our members, stakeholders, and employees.

ERMD is participating in the United States National Institute of Standards and Technology (NIST) working group to develop privacy engineering standards which will guide U.S. organization's decisions regarding resource allocation and effective implementation of controls that decrease privacy risks. ERMD's participation in the development of these NIST standards will result in a closer alignment of the CalPERS Enterprise Privacy Program to future NIST privacy standards.

Additionally, we are implementing automated capabilities that will be used to deliver new and improved information security services to CalPERS. Specifically, the system allows Data Owners to update their classifications (data type, quality, and retention period) on-line. The new system also provides dashboards to data owners, management, and the Information Security Management Section that improves the day-to-day management and monitoring of information assets.

To measure the effectiveness of our current security measures, ERMD is conducting a comprehensive assurance analysis of the current CalPERS information technology infrastructure. This will determine if there are any detectible information security threats to CalPERS electronic information or information technology operational capability. It is being performed independently by a nationally recognized company which specializes in the detection of information security threats. The outcomes of this analysis will be used to inform future information security initiatives.

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 that provides assurance in the safeguarding of our information assets.
- 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 the establishment of an enterprise policy lifecycle management framework.
- 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