Risk & Audit Committee

California Public Employees' Retirement System

Consent

Agenda Item 4e

June 17, 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 January 1 through March 31, 2014[1].

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, an appropriate risk response, develops internal control activities, and continuously monitors and reviews the risks. ERMD serves as a trusted advisor to CalPERS and its business partners on enterprise-wide risks, information security, privacy, HIPAA, business continuity and provides administrative oversight of administrative policies and procedures. ERMD creates and administers information security and HIPAA policies; conducts and reports on enterprise-wide risk assessments, administers and coordinates policy governance,

[1] As a result of the transition to quarterly reporting, activities performed during this period and previously reported to Committee in March have not been duplicated.

provides awareness training (risk, privacy, information security, and business continuity), and facilitates the business continuity program.

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.

Projects

An enterprise governance, risk and compliance (eGRC) system application (RSA Archer eGRC Solutions) is being implemented in multiple phases to automate, integrate and align the following functions:

- Policy Management (Phase 2)
- Compliance Management (Phase 1)
- Business Continuity Management (Phase 2)
- Risk Management (Phase 1)
- Incident Management (Phase 2)
- Enterprise Management (Phase 1)

A description of the RSA Archer eGRC Solutions is provided as Attachment 1 of this agenda item.

During phase one, the Risk Management, Compliance Management, and Enterprise Management solutions were implemented. The system is configured for the Investment Office (INVO) to manage and report risk and compliance events. These applications were also implemented to automate the workflow for enterprise-wide risk assessments, recalibration of the enterprise risk dashboard, and to perform compliance assessments. The process for data owners to identify and classify their information assets according to confidentiality, integrity, and availability requirements as required by CalPERS Information Security Policies was also automated by ERMD.

The next phase will include Policy Management, Incident Management and Business Continuity Management.

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. First quarter activities include:

- Existing policies were updated into the new policy standardized format and gaps between the current versions and the new standards were identified that the policy owner division will update to be consistent with the new standards. Collaborated with the Enterprise Content Management, SharePoint Initiative, to automate the policy approval process within SharePoint.

- Established a Policy Advisory Council to foster collaboration by engaging key stakeholders from all parts of the organization in the policy development process and to collectively address inefficiencies.

- Conducted an analysis of CalPERS top risks to existing policies to identify potential gaps between risk, policy and compliance. ERMD will begin working with the risk owners to report on findings and provide recommendations to address the gaps.

- Developed a communication plan and training plan 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.

- In response to a revision of the California State Information Security Policies (SAM 5300), ERMD updated the Information Security Policies and Control Standards. The Security Policies and Practices were incorporated into the Enterprise Governance Risk and Compliance (eGRC) solution.

Information Security Roadmap

ERMD provides direction, oversight, and serves as a trusted advisor to the Information Security Roadmap Program (ISRP). CalPERS business requirements, laws/regulations, and best practices have been analyzed to create new Information Security Policies and Control Standards which are necessary to govern the enhanced information security capabilities the ISRP projects deliver. ERMD monitors implementation of new ISRP operational processes to verify compliance with Information Security Policies and Control Standards.

ERMD and the Information Technology Services Branch previously identified the need to implement information security controls as recommended by the National Institute of Standards and Technology. Implementation of the new security controls enhances security, reduces risk, and protects our systems. ERMD monitors and reports to the Enterprise Risk Management Committee on implementation of the new security controls.

Strategic Risk Measures

In collaboration with Enterprise Strategic Planning Division (ESPD), ERMD continues to develop strategic key risk indicators (KRIs) to measure and monitor risk proactively. To identify best practices, key risk indicators (KRIs) used by public pension plans to monitor events and trends that may impact achievement of goals and objectives, or increase risk to the system are being researched. This also includes research into how organizations are designing, monitoring, and reporting to

improve risk-informed decisions. This information will be used to develop the KRIs for consideration by CalPERS.

Privacy and Information Security Oversight

ERMD enhanced the HIPAA Privacy program to address new CalPERS, State, and US privacy requirements by SAM 5300. CalPERS health plan business partners are required to sign a Business Associate Agreement (BAA) agreeing to security and privacy terms and conditions before they can access Personal Health Information (PHI). In conjunction with the CalPERS Legal Office and the Health Plan Administration Division, the CalPERS BAA have been updated with the appropriate security and privacy terms.

ERMD worked with the CalPERS Identity Access Management (CalIAM) project to implement a new risk based fraud detection capability for the my|CalPERS system. This capability provides better detective and preventative controls to thwart unauthorized access to a CalPERS' member information.

Business Continuity Management

ERMD completed an analysis of CalPERS business continuity plans to verify compliance with Cal Office of Emergency Services (CALOES) standards. ERMD continues to work with the Division Chief Council and Information Technology Services Branch to ensure consistency between business continuity planning and the 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. ERMD is working with all Division Chiefs to evaluate business continuity plans and identify core critical functions for development of enterprise business resumption priorities.

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). ERMD completed an EOC resource inventory analysis and facilitated the updating and development of "Grab Boxes" that contain tools and unique resources to support critical functions in Division Business Continuity Plans.

Annual Risk Assessment Plan

As outlined in the FY 2013-14 Annual Risk Assessment Plan, a risk assessment was conducted to assess compliance with CalPERS information security policies and standards for the Human Resources Division, Investment Office, and the Enterprise Compliance Division.

ERMD also initiated a risk assessment of Cloud Computing Services in response to an audit finding on this topic. ERMD 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, ERMD is participating in a

workgroup to develop and recommend an appropriate cloud computing strategy and governance policy. ERMD has created a Policy and 139 Control Standards to govern the use of Cloud Computing Services at CalPERS. This will provide a foundation that CalPERS information technology and business areas will use to manage the benefits and risks associated with cloud computing.

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
Attachment 1 – RSA Archer eGRC Solutions

LARRY JENSEN, Chief Risk Officer
Enterprise Risk Management Division

KATHLEEN K. WEBB
Chief Risk and Compliance Officer

CHERYL EASON
Chief Financial Officer