



Consent

Agenda Item 4d

November 19, 2013

ITEM NAME: Enterprise Risk Management Division Status Report

PROGRAM: Risk Management

ITEM TYPE: Consent Information

EXECUTIVE SUMMARY

This reporting item provides a current status update of key activities and accomplishments of the Enterprise Risk Management Division (ERMD), as of October 15, 2013.

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 implementing the following 2013-15 Business Plan initiatives:

- Information Security Roadmap – ERMD provides risk assessment, policy guidance, and recommends control standards, and processes to enhance security measures designed to protect information assets and reduce information security risk.
- Policy Management – ERMD is developing a policy management framework to establish an enterprise-wide oversight approach for managing internal policies and compliance function. To further promote risk management and compliance within CalPERS, ERMD has now fully staffed the new policy management unit.
- Strategic Risk Measures – ERMD is coordinating with the Enterprise Strategic Planning Division (ESPD) in the development of risk indicators for the strategic measures to support achievement of the CalPERS Strategic Plan Goals and Objectives.

BACKGROUND

As part of the CalPERS Integrated Assurance Model, the ERMD conducts risk assessments, promotes risk awareness, provides assurance regarding information security policies, conducts a privacy program, and facilitates emergency management activities.

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. CalPERS Board of Administration (Board) approved Fiscal Year (FY) 2013-14 Annual Risk Assessment Plan outlines the specific risk assessments to be performed along with an allocation of resources for ad hoc requests.

ANALYSIS

The following topics were addressed during this reporting period to further mature the risk management processes 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 for the six Information Security Roadmap Program (SRP) Phase 2 projects. This is a multiyear series of individual projects that will reduce the risk to the confidentiality, integrity, and availability of CalPERS information assets. ISMS is now working with other stakeholders on the execution of SRP Phase 2 which includes the following projects:

- Network Access Control,
- Remote Access Assessment,
- Patch Management,
- Data Loss Prevention,
- eDiscovery, and
- Identity Management.

As a trusted advisor, ISMS provides guidance and assessments in its role as the second line of defense for information security integrated assurance. ISMS created new Security Policies and Control Standards necessary to govern the SRP Phase 2 projects and technologies to ensure the projects conform to current CalPERS Information Security Policies and industry best practices to protect CalPERS information assets. These measures include:

- Examining electronic files to discover confidential information that requires better governance and controls,
- Blocking unauthorized devices from connecting to the CalPERS network,
- Managing hundreds of security updates to thousands of components in the information technology infrastructure which includes all CalPERS laptops, workstations, and mobile devices, and
- Implementing new technology that will increase the maturity of CalPERS legal eDiscovery processes resulting in cost reductions and many other benefits.

ISMS also created new information security awareness training to support the SRP Phase 2 Data Loss Prevention project. This awareness training is focused on increasing CalPERS staff's understanding of the value of protecting CalPERS

information. This new awareness training is integrated into the required ISMS annual information security awareness training.

Work has already started on Phase 3 of the SRP that will be executed in FY 2014-15. Together with other stakeholders ISMS participated in a risk assessment to identify what projects need to be executed during the SRP Phase 3. This enables the project team to identify and prioritize projects in response to evolving information security threats and risks. ISMS and Information Technology Services Branch are currently preparing budget requests to support those Phase 3 projects that are being proposed for completion in FY 2014-15.

Policy Management

To implement 2013-15 Business Plan initiative for Policy Management, ERMD has created a new Enterprise Policy Administration Section (EPAS) and completed recruitment of staff to support development of a policy 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, and a proposed governance process for the management of enterprise policies. The Division Chief Council reviewed the draft policy and it will be presented to executive staff for final review and approval during the second quarter.

EPAS is creating a communication plan and training plan to promote awareness of the new policy framework. These plans will be fully implemented by June 2014, consistent with the Business Plan. Additionally, EPAS has begun identifying authoritative sources and control standards for existing policies to enhance compliance monitoring.

In advance of stable industry standards in September 2013 ISMS identified those CalPERS information security Policy/Control Standards that enable CalPERS information security governance for "Bring Your Own Device (BYOD)". ISMS predicts that industry standards for BYOD will stabilize during FY 2013-14 and then ISMS will select and adopt the industry defined standards by June 2014.

Strategic Risk Measures

ERMD is coordinating ESPD in the development of risk indicators for the Board approved strategic measures to support achievement of the CalPERS Strategic Plan Goals and Objectives. The risk indicators are designed to prevent variability from anticipated performance and achievement of the Strategic Plan Goals and Objectives. ERMD will continue to collaborate with ESPD on the development of these strategic risk measures.

Annual Risk Assessment Plan

The Risk Assessment and Intelligence Section (RAIS) are performing the risk assessments as outlined in the FY 2013-14 Annual Risk Assessment Plan.

Specifically, RAIS began conducting risk assessments for the following risk domains and developed risk registers to support the domain ratings:

- Pension Funding,
- Human Resources Management,
- Municipal Bankruptcy, and
- Pension Reform Implementation.

An information security risk assessment was also initiated by the Enterprise Compliance Division to assess compliance with CalPERS information security policies and standards.

RAIS is conducting a risk assessment of Cloud Computing Services in response to an audit finding on this topic. In August 2013, ISMS adopted the industry standards for “cloud computing” defined by the Cloud Security Alliance. Subsequently in September 2013, the CalPERS information security Policy/Control Standards were updated to govern CalPERS adoption of “cloud computing” to support the risk assessment.

These assessments are conducted jointly with executive and division management further supporting the cultivation of a high-performing, risk intelligent and innovative organization. The Enterprise Risk Dashboard will be updated to reflect the results of these risk assessments.

To further promote the strategic goal to “Cultivate a high performing, risk intelligent and innovative organization”, ERMD provided a series of progressive training to the Division Chief Council regarding risk governance, risk identification, and risk assessment. The Division Chiefs performed a more active role in risk governance, development of risk registers, emerging risk reports, top risk reports, and recalibrated the Enterprise Risk Dashboard. This initiative is planned to be fully integrated by end of FY 2013-14 second quarter.

Training and Awareness

To cultivate a risk intelligent culture, RAIS continues with its internal Governance Risk and Compliance (GRC) training program for staff development. This training program commenced June 2013 and will be completed this month.

ISMS completed a refresh of the current information security awareness training to both reflect new information security risks and technologies. This refreshed training will be available to all CalPERS staff this month and delivered during their mandatory annual information security awareness training throughout the remaining months of FY 2013-14.

Emergency Management

The Emergency Management (EMAN) unit assisted in conducting a full-scale offsite evacuation drill to Crocker Park to increase awareness and training in the event of an

actual emergency or disaster. The Floor Warden and Emergency response teams were activated to test and evaluate segments of the CalPERS Emergency Response Plan. EMAN is evaluating lessons learned from the offsite drill to make improvements to CalPERS emergency response plans.

Additionally, CalPERS joined over 9 million Californians in the Great Shakeout drill, a simulated earthquake-based disaster.

EMAN also completed a review and analysis of the updated Business Continuity Plans for each division. A draft Business Impact Analysis and Gap Analysis was completed to identify opportunities for improvement, primarily in alignment of the plans. EMAN will continue working with management to update the plans to ensure proper alignment and address any gaps between the plans. The Business Continuity Plans are critical to ensure all operations are up and running at full capacity in the event of a major incident.

Projects

eGRC Platform - To improve efficiency, an Enterprise Governance Risk and Compliance (eGRC) solution is being implemented to automate certain risk management, compliance, incident management, business continuity, and policy management functions. During this reporting period, the business use cases were prioritized and a roadmap and blueprint for implementing the solution was developed. Phase I will focus on automating the enterprise risk dashboard and the supporting risk registers, incident management, and standardizing compliance assessments.

The ERMD eGRC initiative provides additional capabilities that ISMS will use to deliver new and improved information security services to CalPERS. Specifically, ISMS created twelve use cases to expand the current data classification program that will include aspects of data quality. These use cases were submitted to the eGRC project team in September 2013 and currently planned to be implemented by June 2014.

My|CalPERS Access Project - ISMS is working with other stakeholders to update the my|CalPERS system so that staff can access only those functions necessary to perform their specific job duties. All CalPERS divisions have been contacted and their identification of the required my|CalPERS functions to support their business processes was completed. Some changes were made to my|CalPERS during the 3rd quarter of FY 2013-14 and others are scheduled to be completed by the end of FY 2013-14 which strengthens security by limiting access to confidential and sensitive member information.

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, Risk Officer
Enterprise Risk Management Division

KATHLEEN K. WEBB
Chief Risk and Compliance Officer

CHERYL EASON
Chief Financial Officer