



## Consent

### Agenda Item 4c

September 17, 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 August 31, 2013.

#### **STRATEGIC PLAN**

This agenda item supports Strategic Plan Goal B: Cultivate a high-performing, risk-intelligent and innovative organization.

#### **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. To further promote risk management and compliance within CalPERS, ERMD is also implementing a new policy management unit.

An effective enterprise-wide risk management provides a holistic approach to the identification of organizational risks, creates an appropriate risk response, develops internal controls, and continuously monitors and reviews the risks. ERMD also strives to integrate risk management into the organization, at both the strategic and operational levels.

#### **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.

#### Risk Assessments

The Risk Assessment and Intelligence Section (RAIS) continues to perform the risk assessments as outlined in the FY2013-14 Annual Risk Assessment Plan. These assessments are conducted jointly with executive and division management further supporting the cultivation of a high-performing, risk intelligent and innovative organization. For this first quarter, RAIS completed a risk assessment for the Supplemental Income Plan and started the discovery phase for a risk assessment of

Cloud Computing. RAIS has also initiated the Pension Funding and Human Resources Management risk assessments as provided in the Annual Risk Assessment Plan. Final Reports will be prepared for the Executive Risk Management Committee and the Division Chief Council (DCC). The Enterprise Risk Dashboard will also be updated to reflect the results of the assessments and mitigation efforts.

RAIS continues performing the Information Security Risk Assessments as outlined in the FY2013-14 Annual Risk Assessment Plan. Final reports are being prepared for management of the division to respond to the risks identified in the reports. The Enterprise Risk Dashboard will be updated to reflect the results of these risk assessment results and mitigation efforts.

To further promote the strategic goal to “Cultivate a high performing, risk intelligent and innovative organization”, ERMD is integrating enterprise risk management and exposure report updates to the Division Chief Council. Division Chiefs will take a more active role in the development and assessment of the risk domain registers, emerging risk reports, enterprise risk management dashboard, and top risk reports. Final reports will be presented to the Executive Risk Management Committee for their review and input on actions required to achieve Strategic Plan goals and Business Plan objectives. This initiative is planned to be fully integrated by end of FY2013-14 second quarter.

RAIS continues to work with the program areas to address risk mitigation strategies identified in the top risk report. Additionally, RAIS is working with the Business Plan objective owners to identify risks that may prevent the achievement of objectives at the onset of the business planning process. To provide executive management and the board with reasonable assurance regarding the management of risks to achieve the business plan objectives, RAIS will review the status of each business plan objective after the second and fourth quarters annually.

#### Risk Awareness

To cultivate a risk intelligent culture, RAIS continues with its internal Governance Risk and Compliance (GRC) training program for staff development and certification. This training program commenced June 2013 and will be completed in November 2013. ERMD will then review the program as a potential offering to other departments within CalPERS.

#### eGRC Platform

An Enterprise Governance Risk and Compliance (eGRC) solution is being implemented to automate enterprise risk management, compliance management, incident management, business continuity management, and policy management functions. A governance committee, with the CORCE as the executive sponsor, was developed to guide implementation of the automated solution. Currently, OERM is in the discovery phase documenting “as-is” processes and determining the “to-be” state to understand opportunities to mature the programs, process improvements, and

enhancements. An eGRC Blueprint and Roadmap based upon best practices is being developed for deployment of the automated solution.

#### Information Security Strategy, Planning and Policy

Information Security Policies are regularly created to provide guidance to CalPERS staff and used as a basis for the measurement of activities related to the protection of CalPERS information assets. These Information Security Policies support the operational integrity of the CalPERS information technology infrastructure and the confidentiality, integrity, and availability of CalPERS information assets. They also enable CalPERS to be in compliance with multiple laws and regulations which include the California Government Code and HIPAA.

A governance process for approving new Information Security Policies has been approved by the Information Technology Services Branch and is being integrated into the CalPERS enterprise policy governance process and framework, which aligns with our efforts to implement an Integrated Assurances Model.

The Information Security Management Section (ISMS) is co-sponsoring a task force that is reviewing CalPERS staff access to my|CalPERS functions and the processes that control access to the system. Phase 2 activities for FY13/14 are underway and are focused on improving the separation of duties for my|CalPERS functions. Properly aligning the staff's access to my|CalPERS functions with the business processes they perform will reduce the risk of compromises to both the confidentiality and integrity of CalPERS information.

#### Information Security Technology Assurance

Active engagement and coordination with CalPERS information technology groups continues. This cooperation provides both a separation of duties and integrated assurance that Information Security Policies are being followed and results in better confidentiality, integrity, and availability of CalPERS information assets.

The FY12/13 Information Security Roadmap Program (SRP) projects have been successfully completed. Among them was the implementation of a new CalPERS workstation computer baseline configuration which is based on the United State Government Computer Baseline standard (USGCB). Over 3,000 workstation computers were updated to meet the enhanced security standard. The implementation of this baseline significantly reduces the risk that hackers could control CalPERS computer workstations enabling them to steal information and disrupt CalPERS operations.

Work has started on Phase 2 of the Information Security Roadmap Program (SRP) for FY13/14. These SRP projects include major initiatives addressing the retention and exchange of digital information subject to discovery in litigation ( eDiscovery), Identity and Access Management, and Data Loss Prevention. All of these SRP projects have been selected based upon an annual information security risk assessment to improve the protection of CalPERS information assets.

### Information Security Privacy & Awareness

The redesign and implementation of the OERM website on the CalPERS intranet (Inside CalPERS) was completed. This has consolidated separate intranet sites for Risk, Compliance, Information Security, HIPAA, and Emergency Management into a single presence on Inside CalPERS that will present a complete view of OERM to CalPERS staff.

The information security component of the New Employee Orientation and LEADER training has undergone a significant revision to improve both the training experience and the application of learned behaviors. The information security training has been changed to use a case study-based learning model because research has shown this approach gets the learner involved and encourages their immediate use of newly acquired skills. Ultimately the application of the newly learned information security skills will enable CalPERS staff to better protect CalPERS information assets.

### Information Security Incident Management

When information security events happen, the CalPERS response is coordinated across all affected CalPERS groups. In compliance with California laws and policies, if an event is elevated to the status of an incident, it is reported to the California Information Security Office (CA ISO) and the California Highway Patrol (CHP).

The design and planning of a new automated incident management tool is underway. It will incorporate information security incident risk reporting into the CalPERS eGRC solution. This will automatically include risks associated with information security incidents in the eGRC risk reports and dashboards enabling CalPERS management to consider the impact of information security incidents when making decisions regarding CalPERS programs, projects, and operations.

A secondary responsibility of the IS Incident Management group was to support investigations by the Legal Office (LEGO) and Human Resources Support Division (HRSD). Because all CalPERS investigative activities are being consolidated into the Legal Office (LEGO) the IS Incident Management group has transferred its investigative functions to LEGO.

### Emergency Management

The Emergency Management unit assists all CalPERS divisions in the preparation and execution of emergency functions to ensure the safety of CalPERS staff and resumption of CalPERS operations disrupted by natural, technological, or human created hazards. There are 3 key activities being planned that will increase awareness and training in the event of actual emergency or disaster impacting CalPERS to ensure all operations are up and running at full capacity in the event of a major incident. Planning is underway for all the following activities in the next quarter.

- An Emergency Operations Center (EOC) Tour to familiarize new and existing leadership with the EOC and obtain a high level overview of the EOC activation plan.
- A full-scale Offsite Evacuation Drill to Crocker Park. The Floor Warden and Emergency response teams will be activated in response to a simulated

earthquake-based disaster. This evacuation drill will allow us to test and evaluate segments of the CalPERS Emergency Response Plan.

- Incident Command Structure (ICS) Training at the EOC. The purpose is to train key staff in their roles and responsibilities using ICS planning operations in the event the EOC is ever activated.

### Enterprise Policy

To promote a risk intelligent organization, a central repository and governance adoption processes are being developed that will be used by the enterprise for the documentation and maintenance of all current policy statements that are intended to govern behavior by all those serve as CalPERS employees, managers, executives, contract resources and business partners.

ERMD is establishing a new enterprise-wide policy administration unit that is responsible for the following:

- Implementing and maintaining a policy “life-cycle” governance process that defines how a policy is created, maintained and retired.
- Increase policy awareness by notifying impacted staff when an existing policy is updated or a new policy has been adopted.
- Establish a governance process that will facilitate the identification and maintenance of measurable policy statements / control standards.
- Establish a single central repository containing all approved and fully adopted policies and the associated policy statements / control standards where authorized users can read, research, cross-reference and print materials in a user friendly and user intuitive manner.

A draft policy, tools, and a proposed governance process for the administration of enterprise policies was developed and reviewed by the Division Chief Council. It will be presented to executive staff for final review and approval during the second quarter.

As approved in the FY 2013-14 budget, recruitment for two positions is underway to staff the new unit. The best practices for implementing an enterprise policy management unit were researched and planning documents were developed to implement the new enterprise-wide policy administration management unit.

### **BUDGET AND FISCAL IMPACTS**

Resources for the initiatives outlined in this ERMD status report are funded by existing internal resources or funds were requested through the annual budget planning process. No additional funds are being requested at this time. The eGRC solution is currently budgeted at \$488K and is included in the current fiscal year budget. Staff will perform work related to discovery, design, configuration, and implementation of the automated solution.

---

LARRY JENSEN, Risk Officer  
Enterprise Risk Management Division

---

KATHLEEN K. WEBB  
Chief Officer of Risk, Compliance and Ethics

---

CHERYL EASON  
Chief Financial Officer