

Enterprise Risk Management Division
May 2012

Board Assignment Status

| Assignment Date | Request / Subject | Due Date | Status / Completed Date |
|-----------------|------------------------------|----------|-------------------------|
| | No current board assignments | | |

Other Items of Interest

| Item of Interest | Status / Completed Date |
|-----------------------------|---|
| Personal Trading Regulation | <p>The proposed personal trading regulations were published by the Office of Administrative Law on March 30, 2012. The public comment period ended May 14, 2012 and a public hearing will be held at the June Board of Administration meeting.</p> <p>Compliance 11 was selected as the vendor for the personal trading system. Contract negotiations and implementation plans are underway.</p> |
| Risk Assessments | <p>Facilitated update of the Enterprise Risk Management Dashboard and Top Risk mitigation strategies.</p> <p>Reviewed the status of six compliance risk assessment reports dating back to January 2009 with the Investment Office to determine the status of 42 issues identified in the reports. Determined 30 issues were fully resolved and 12 issues remain open. Established a process to periodically follow up on issues and to assist the Investment Office with resolution.</p> <p>Reviewed the status of ten information security risk assessment reports and identified five common enterprise information security risks. Detailed reports will be prepared for management to address the unresolved risks identified in the reports.</p> |

| Item of Interest | Status / Completed Date |
|-------------------------------|---|
| Strategy, Planning and Policy | <p>The Information Security Management Section (ISMS) and ITSB have created a joint Information Security Roadmap that identifies a phase implementation of information security initiatives that will be implemented over the next 5 years. In preparation for the FY12/13 implementation ISMS and ITSB have begun implementation planning, resource allocation, and staffing activities.</p> <p>Both the structure and content of CalPERS information security policies have been updated to enable us to better align them with major regulatory (HIPAA, SOX, etc.) requirements and industry standards (NIST, ISO, COBIT, etc.).</p> <p>A new automated tool is being implemented that provides a foundation for a best-in-class policy program. It enables a comprehensive and consistent process for managing the lifecycle of policies and will enable us to better communicate policies to CalPERS staff, request, and track their acceptance, and manage any exceptions. The pilot for the implementation of this automated tool has been rescheduled to calendar 2Q2012 (from 1Q2012) without affecting the implementation date of calendar 4Q2012.</p> <p>The following information security practices have been published:</p> <ul style="list-style-type: none"> • Electronic Messaging Record Management (new) • Life Cycle Risk Management Practice (new) • Identity Authentication Practice (revised) |
| IT Control and Compliance | <p>A tool used by ISMS to monitor the compliance of information technology systems has been implemented. This IT compliance tool enables the measurement of 100+ security characteristics of CalPERS information technology systems and user accounts. New compliance measurements are being planned and will be continuously implemented over time. The following measurements have been implemented during the last month:</p> <ul style="list-style-type: none"> • Password compliance to CalPERS policies and standards • Administrator Rights to Workstations <p>During the most recent reporting period the ISMS and ITSB reviewed and took appropriate action on 8 US-CERT Technical Cyber Security Alerts issued by the National Cyber Alert System.</p> |
| Privacy and Awareness | <p>The vendor that will provide the content for the updated information security awareness training has been selected. The content they provide meets numerous standards and compliance requirements including PCI DSS, HIPAA, FISMA, ISO 27001, and FERPA. It is widely used by both the Fortune 500 and government agencies.</p> |

| Item of Interest | Status / Completed Date |
|-------------------------------|---|
| | A framework is being developed that will provide the basis for the ISMS privacy program. It is being based upon privacy laws and regulations, policies, best practices, and experiences by other organizations. |
| IT Investigations (Incidents) | See Attachment 4c – A1 – Internal See Attachment 4c – A2 - External |