Enterprise Risk Management Division
October 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
Risk Assessments	Facilitated update of the Enterprise Risk Management Dashboard and Top Risk mitigation strategies. 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.
Risk Assessments (continued)	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.
Strategy, Planning and Policy	The first five initiatives of the ERMD/ITSB Information Security Roadmap that were scheduled to start in FY12/13 are underway. The project charters have been approved by CalPERS Executive Management and project planning has commenced. These initiatives are part of the continuous improvement to

Item of Interest	Status / Completed Date
	CalPERS information security capabilities that is needed to meet today's information security challenges. The updated CalPERS information security policies are completed and are being approved in phases. When they are approved and implemented CalPERS will be in alignment with the major regulatory (HIPAA, SOX, etc.) requirements and industry standards (NIST, ISO, COBIT, etc.). The pilot is underway for a new automated tool to better organize and manage the information security policy lifecycle.
IT Control and Compliance	The scope of the automated tool used by ISMS to monitor the compliance of information technology systems to information security is being expanded to measure additional types of systems. It is also being used in the Information Security Roadmap to measure and validate the improvements that are being implemented.
Privacy and Awareness	The update to information security awareness training has been completed and will be released to all staff in October 2012. The content 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. This new information security awareness training is also ADA compliant
IT Investigations IT Investigations (continued)	New protocols have been implemented to supplement the coordination and reporting of information security investigations. Improvements to the tools and processes ERMD uses to support legal perseveration and production (eDiscovery) requests are being planned.