

**ENTERPRISE RISK MANAGEMENT DIVISION
As of May 15, 2013**

	Item of Interest	Status/Completed Date
1	Risk Assessments	<p>The Enterprise Risk Management Division (ERMD) completed an enterprise-wide risk assessment, conducted jointly with the Office of Audit Services, to update the Enterprise Risk Management Dashboard and Top Risk Report. Risk assessment results were presented to the Executive Risk Management Committee and the Division Chief Council. The Enterprise Risk Dashboard was revised to reflect the current risk landscape. New Board reports were developed for top risks. The Risk exposure reports will be presented to the Risk and Audit Committee at the June meeting (Agenda Item 9a) and capture the results of the enterprise-wide risk assessment.</p> <p>ERMD also completed a risk assessment of the FY 2012-14 Business Plan objectives scheduled for completion by June 30, 2013. The Action Plan owner identified and assessed risks that may prevent them from achieving the Business Plan objective within the required timeframe. All risks identified will continue to be monitored and mitigated as necessary to achieve the Business Plan objectives.</p> <p>The municipality bankruptcy risk register was updated to reflect current risk responses. On-going assessment to be completed and reported to Executive Staff to assist monitoring the risks and developing risk responses.</p> <p>Continued Board approved Information Security Risk Assessments with designated divisions. Final reports to be prepared for management to address the unresolved risks identified in the reports.</p> <p>The ERMD is continuing to work with the program areas to address risk mitigation strategies identified in the Top Risk Report.</p>
2	Risk Awareness	<p>Developing internal Governance Risk and Compliance (GRC) training program for staff development and certification. Training program to commence June 2013.</p> <p>Continuing Enterprise Risk Management (ERM) / GRC awareness program for the Board of Administration and Executive Staff. Next sessions will be conducted in September and/or November.</p>

<p>3</p>	<p>IS Strategy, Planning and Policy</p>	<p>The IS Strategy, Planning and Policy group is working as part of a task force to review CalPERS staff access to my CalPERS functions and the processes that control access to the system. Some processes have been revised to better control how access is requested and authorized. An analysis of the specific access required for staff to perform their job duties is underway and any access beyond what is necessary is being removed.</p> <p>A governance process for approving new Information Security Policies and Control Standards has been created and is pending approval by the stakeholders and executive management.</p> <p>The analysis and approval by the ITSB Enterprise Architecture Board (EAB) of the new information security Control Standards that affect ITSB continues. The 17 Information Security Policies and 534 new Control Standards establish a framework that better aligns CalPERS Information Security Policies with industry standards and regulations that include HIPAA, HiITECH, and NIST. The EAB has approved 254 new Control Standards and another 26 are pending review and approval by the EAB.</p> <p>All Information Security Policies and 67 Control Standards that support the FY12/13 ERMD/ITSB Information Security Roadmap projects have been completed and approved. An additional 34 Control Standards governing specific characteristics of the Roadmap projects are currently under development or pending approval.</p> <p>The pilot for the automated tool that will better organize and manage the information security policy lifecycle is underway.</p>
<p>4</p>	<p>IS Technology Assurance</p>	<p>Close cooperation with ITSB continues to support the Information Security Roadmap Program FY12/13 projects to assure that information security aligns with the CalPERS business interests. Oversight of the implementation of the new computer workstation baseline configuration (USGCB) continues and 251 configuration items have been approved and implemented. An additional 287 configuration items are either approved or under analysis.</p>
<p>5</p>	<p>IS Privacy & Awareness</p>	<p>The redesign and implementation of the Office of Enterprise Risk Management (OERM) Insider site is underway. This will consolidate separate Insider sites for Risk, Compliance, Information Security, HIPAA, and Emergency Management into a single Insider presence that will present a complete view of OERM to CalPERS staff.</p> <p>The LEADER and New Employee Orientation training has been updated to consolidate all of the OERM related training.</p>

<p>6</p>	<p>IS Incident Management</p>	<p>The primary responsibility of the IS Incident Management group is to receive reports of information security issues and coordinate our response. Incoming information security reports are initially classified as Events but can be upgraded to Incidents depending upon their severity and the legal reporting requirements. Security Events are often issues reported by business partners who are independently handling the issue. However, Incidents involve the disclosure of member information which requires that we notify the member and also report the Incident to the California Information Security Office (CA ISO) and the California Highway Patrol (CHP). During the last two months the IS Incident Management group has responded to seven information security Incidents and nine External (includes HIPAA) Events. In addition, this group monitors security alerts issued by multiple cyber security organization which include the Multi-State Information and Analysis Center (MS-ISAC) and the National Cyber Awareness System (US-CERT). During the past two months it has reviewed and taken appropriate action on 31 of these alerts.</p> <p>During the past two months this group has also provided technical support for multiple investigations conducted by the CalPERS Legal Office and Human Resources Division.</p>
<p>7</p>	<p>Emergency Management</p>	<p>The Business Impact Analysis is complete and a Gap Analysis was developed. The Division Business Continuity Plans are being updated to close the gaps identified and align with the Disaster Recovery Plan.</p> <p>Planning is underway for a preparedness exercise involving activation of the emergency operations center.</p> <p>A review of automated solutions to support business continuity and disaster recovery is being conducted.</p>
<p>8</p>	<p>Enterprise Policy</p>	<p>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.</p>

	Enterprise Policy (cont.)	<p>A central policy library software solution was selected and implemented which serves as the policy repository and life cycle management tool. Over 250 formally recognized and adopted CalPERS policies were uploaded into the repository. 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.</p> <p>A draft Meta Policy and tools for creating enterprise policy were developed along with a proposed governance process for creating, approving, and implementing policies.</p>
--	---------------------------	--