CALSTRS

Audits and Risk Management Committee

Item number 3 – Open session

Subject: FY 2025-26 Enterprise Risk Management & Compliance Services Maturity Plan Closeout Report

Presenter(s): Chairperson

Item type: Consent information

Date and time: September 24, 2026 – 0 minutes

Attachment(s): Attachment 1 – Enterprise Risk Management Maturity Plan Closeout Report

Attachment 2 – Enterprise Compliance Services Maturity Plan Closeout Report

---

Item purpose

The purpose of this item is to provide the Audits and Risk Management (ARM) Committee with a closeout report on the Enterprise Risk Management (ERM) and Enterprise Compliance Services (ECS) maturity plans. These plans cover the period of July 1, 2025, through June 30, 2026. The maturity plans were developed in support of CalSTRS Strategic Plan Goal 3, Objective C: Mature how risks are defined, viewed and managed.

Recommendation

This is an information item only.

Executive summary

The ERM and ECS FY 2025-26 maturity plans focused on strengthening risk management, compliance practices and enterprise-wide coordination. Key accomplishments include implementing new enterprise risk and policy management software, standardizing risk and compliance processes, and enhancing alignment with strategic planning and assurance partners.

Enterprise Risk Management (ERM)

Over the past year, the ERM team focused on maturing foundational processes and establishing an integrated approach to risk oversight. Attachment 1 to this item outlines the progress made under the FY 2025-26 ERM maturity plan, which includes:

- **Deployment of an enterprise risk software platform Riskonnect**
  Implementing the Riskonnect software provides CalSTRS with standardized, enterprise-wide risk analysis and reporting. This modernized infrastructure increases efficiency, improves data integrity, and ensures leadership has timely, accurate insight into emerging risks—an essential capability for safeguarding the long-term health of the fund. ERM staff is actively using Riskonnect to gather risk data and generate reports. System access for executives, risk champions, and other assurance functions will be granted once training is completed and procedures are developed to help new users navigate the system.

- **Integration of organizational risk data**
  Consolidating risk information into one system enables clearer visibility into enterprise risk trends, strengthens consistency in reporting, and creates a shared foundation for decision-making across business areas. This integrated view ensures that CalSTRS can anticipate issues early and respond strategically.

- **Alignment with Enterprise Strategy Management**
  Our new enterprise risk management software enables linking our strategic plan initiatives directly to our enterprise risks so they can be monitored through this lens. Connecting ERM processes with strategic planning supports data-driven organizational decisions. This alignment helps identify key risk indicators and tolerances, ensuring that risk considerations are embedded into strategic priorities and long-term planning.

- **Unified, cross functional approach to risk evaluation**
  ERM strengthened collaboration with assurance partners by coordinating our annual ERM, Audit Services, and Enterprise Compliance risk assessments into one process. This allows for improved transparency and risk coordination across the organization. This unified approach helps eliminate gaps, reduces duplication and enhances CalSTRS' resilience against enterprise-wide risks.

Collectively, these achievements demonstrate a meaningful shift toward a more mature, systematic and collaborative enterprise risk environment—one that supports prudent stewardship and long-term stability. Some planned activities were not completed because the Riskonnect implementation took longer than expected. Activities that were not completed included developing new KRI's, establishing priorities for risks, and creating performance metrics. These activities were incorporated into the FY 2026-27 work plan.

Enterprise Compliance Services (ECS)
The ECS program advanced key compliance components that reinforce CalSTRS' ethical standards and protect the organization's credibility—critical pillars of member trust. Attachment 2 to this item outlines the progress made on the FY 2025-26 ECS maturity plan, which includes:

- **Piloting and launching the risk-based policy review cycle**
  A "risk-based policy review cycle" means policies are reviewed according to how much

risk they pose to the organization. High-risk policies are examined annually, while those considered low-risk are scheduled for review every two or three years. This approach reduces unnecessary workload for staff by focusing attention where it's needed most. Moving to a risk-based review model, instead of reviewing all policies annually, improves policy governance by focusing attention where risk exposure is greatest. This approach makes oversight more efficient, strengthens compliance, and enhances operational consistency across the enterprise. We estimate that this approach saves approximately 500-800 hours of staff time per year.

- **Completing comprehensive enterprise policy reviews**
  As part of our proactive approach to maintaining policy integrity, ECS conducted a targeted review of a specific policy and systematically tested its key attributes for compliance. This process was designed to verify that staff were reasonably following the policy requirements. Through this compliance testing, ECS identified areas where processes could be further strengthened and made recommendations for improvement, directly supporting transparency, accountability, and sound business practices.

- **Launching annual confidentiality acknowledgement**
  A confidentiality acknowledgement is a document that reinforces case manager's understanding of their responsibilities to protect sensitive information that may be submitted through the hotline. By requiring case managers to annually sign a confidentiality agreement, and by standardizing confidentiality education for hotline case managers, ECS reinforces CalSTRS' commitment to protecting sensitive information, supporting a strong reporting culture, and upholding members' trust.

- **Administering policy management education**
  In February 2026, ECS conducted a survey of policy owners to assess organizational training needs and used the findings to develop a comprehensive Policy Owner Handbook. Additionally, ECS formalized workflows and policy owner procedures to provide clear guidance on the policy management framework, determining when a policy is required, how to draft an effective policy, and the appropriate approval channels within CalSTRS. These new tools were provided to all CalSTRS policy owners in June 2026 and are provided to new staff when they are assigned to review policies. Enhancing understanding of policy processes strengthens consistency, reduces compliance risks, and supports the long-term resilience and governance of the organization.

- **Deploying a policy management software module**
  Implementing the system supports centralized oversight and improves CalSTRS' ability to track, manage, and evaluate policies at scale. This infrastructure advances program maturity and underpins a sustainable compliance framework.

In addition to ongoing professional development, both teams continued to build expertise by earning industry-recognized certifications. This year, one staff member obtained an Enterprise Risk Management Certification, another earned the Integrated Risk Management Professional

Certification, and a third achieved the Integrated Compliance and Ethics Certification. These new credentials further strengthen the team's capacity to support CalSTRS' risk and compliance programs. Remaining items—primarily those dependent on full software integration—will continue in the FY 2026-27 work plans. Overall, the maturity plans significantly advanced CalSTRS' risk and compliance capabilities, laying a strong foundation for continued progress.

Background

A maturity assessment conducted by Weaver & Tidwell, LLC was presented to the ARM Committee in March 2023 providing recommendations to mature the ERM and ECS programs. 18-month maturity plans were developed by the ERM and ECS staff and shared with management, business area risk champions, and various stakeholders to gather feedback and foster engagement in strengthening our risk and compliance culture. These plans were presented to the ARM Committee in November 2023 and focused on building and enhancing internal ERM and ECS infrastructure and processes.

With the closeout of the 18-month maturity plan, the FY 2025-26 plans were developed to further advance program maturity. These plans incorporated additional activities designed to proactively identify and address risks, strengthen organizational resilience, and maintain a culture of compliance and ethical behavior.

ERM and ECS have incorporated continuous improvement and program maturity into our annual planning process. As a result, our yearly plans will now be referred to simply as work plans rather than maturity plans. The Enterprise Risk Management and Compliance Services FY 2026-27 work plan was presented to the ARM Committee in March 2026.

Strategic Plan linkage: Goal 1: Trusted stewards – Ensure a well-governed, financially sound trust fund, Objective E: Enhance board practices to evolve excellence in governance, and Goal 3: Sustainable organization, Objective C: Mature how risks are defined, viewed and managed.

Board Policy linkage: Board Governance, Section G. Risk Management Policy

---

Optional reference material:
May 2024 ARM Committee, Item 7 – Enterprise Risk Management and Compliance Services Maturity Plan Progress Report

March 2026 ARM Committee, Item 8 – Enterprise Risk Management and Compliance Services FY 2026-27 Work Plan