CALSTRS

Audits and Risk Management Committee

Item number 8 – Open session

Subject: Enterprise Risk Management Report

Presenter(s): Lynn Bashaw

Item type: Information

Date and time: November 5, 2026 – 15 minutes

Attachment(s): Attachment 1 – Enterprise Risk Score Report

PowerPoint presentation(s): Enterprise Risk Management Report

---

Item purpose

This item presents the enterprise risk management report as of September 30, 2026 to the Audits & Risk Management Committee (ARM Committee) and marks the first report generated using CalSTRS' new enterprise risk management software, Riskonnect. Going forward, staff plans to transition from providing a semi-annual enterprise risk report to providing a risk update at each ARM Committee meeting, enabling more timely and consistent risk reporting on the organization's risk profile. We will continue to provide reporting on these risks through the CEO Report when there is no ARM Committee scheduled. As this is the inaugural report using the new system, staff will continue to refine reporting processes and build additional information and capability into the platform in future cycles, informed by ARM Committee feedback and the organization's growing experience with the tool.

Recommendation

This is an information item only.

Executive summary

Staff will present the updated enterprise risk management approach. The presentation will explain how the approach improves the identification, assessment, and monitoring of enterprise risks; provides more actionable insight through subcategory-level reporting; and supports consistent, timely information for leadership and the ARM Committee. It will also include an overview of artificial intelligence risks and how CalSTRS is managing them through its enterprise risk management framework, with particular focus on cybersecurity, data protection, and vendor management. These enhancements are important to strengthening oversight,

prioritizing mitigation efforts, and ensuring that emerging and significant risks are managed in alignment with CalSTRS' strategic objectives. The following updates highlight how the report is evolving to provide more actionable insight and support continued refinement of the enterprise risk management process:

- **Transition from category-level to subcategory-level reporting.** The ERM report moves away from scoring risk by broad category — which offers limited actionability — toward scoring by subcategory, providing greater detail on where risks are emerging and enabling more precise, targeted mitigation by management. Attachment 1 contains the Enterprise Risk Score Report, which presents the residual risk scores by subcategory. These scores are subject to ongoing calibration and refinement as we further develop our risk taxonomy and scoring methodology. Over time, the scores will continue to evolve to reflect improvements in our assessment practices and organizational experience.

- **Risk mitigation actions.** For the highest-scoring risk subcategories, the report identifies a named risk owner and the specific mitigation actions underway, providing assurance that risks are being actively monitored across the enterprise.

- **Emerging and existential risks.** The report highlights risks on the horizon, including a newly identified emerging risk (post-quantum cryptography) and longer-term existential risks. Emerging risks are developing or evolving risks whose potential impacts, likelihood, or timing may not yet be fully understood. Existential risks have low likelihood but are risks that could fundamentally threaten CalSTRS' ability to achieve its strategic objectives or continue critical operations if they were to materialize. Through the ERM framework, management monitors emerging and existential risks to determine whether these risks warrant inclusion in the enterprise risk profile.

- **Artificial intelligence risk.** An overview of how CalSTRS governs AI risk using the same enterprise risk discipline applied to other risks, with particular focus on cybersecurity, data protection, and third-party/vendor management.

- **Next steps.** Staff will outline ongoing control validation, strategic plan mapping, development of reporting options for the full board, and will seek ARM Committee input on how best to convey this information to its various audiences.

Management is actively monitoring and mitigating enterprise risks. There are no concerns to report at this time.

Strategic Plan linkage: Goal 1: Trusted Stewards — Enhance board practices to evolve excellence in governance. Goal 3: Sustainable Organization—Mature how risks are identified, defined, viewed, and managed.

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

---

Optional reference material: September 2026 ARM Committee Item 9 – Enterprise Risk Reporting Refresh