



Audits & Risk Management Committee

Item Number 5 – Open Session

Subject: Enterprise Risk Management Framework – First Reading

Presenter(s): Julie Underwood and Lynn Bashaw

Item Type: Information

Date & Time: May 2, 2024 – 15 minutes

Attachment(s): Enterprise Risk Management Framework – First Reading

PowerPoint(s): Enterprise Risk Management Framework

Item Purpose

The purpose of this item is to present the Audits and Risk Management Committee with a first reading of the newly documented Enterprise Risk Management (ERM) Framework. While most of the risk and compliance *processes* outlined in this document have been in place for some time, the ERM Framework itself had not been memorialized into one document. CalSTRS commitment to effective risk management begins with the Teachers' Retirement Board's (board) approval of this ERM Framework, which clearly articulates their expectations for managing risk throughout the organization. This item supports the Audits and Risk Management Committee in meeting their responsibility for reviewing and recommending changes to the board to the ERM Framework.

Recommendation

Staff recommends that the Audits and Risk Management Committee consider the proposed Enterprise Risk Management Framework. Staff will incorporate feedback from the Committee into the framework document and bring it back for a second reading unless the Committee decides to approve the recommended charter at this meeting.

Executive Summary

The board delegated oversight of the ERM framework to the Audits and Risk Management Committee through the Audits and Risk Management committee charter. Documenting the ERM framework is vital for our organization's strategic planning and operational decision-making processes and helps the Audits and Risk Management Committee meet its responsibilities for oversight of the ERM framework. An ERM framework provides a structured approach to

identifying, assessing, and managing risks, thereby enhancing our ability to anticipate and mitigate potential threats to our objectives. The CalSTRS ERM Framework is based on the COSO¹ integrated ERM framework and serves as a foundational tool to systematically integrate risk management into our culture, processes, and governance structure. By documenting the ERM framework, we can:

- **Improve risk awareness:** Ensure that all stakeholders have a clear understanding of the organization’s risk landscape and processes.
- **Enhance decision-making:** Enable informed decision-making by considering risk-factors and their potential impact on strategic initiatives and operational activities.
- **Integrate risk and compliance:** Integrate risk management and compliance functions within a unified framework that enables efficiencies and a holistic approach to addressing organizational objectives and regulatory requirements.
- **Strengthen accountability:** Define roles, responsibilities, and accountability for managing risks at various levels of the organization.
- **Facilitate continuous improvement:** Establish a structured framework for monitoring, evaluating, and enhancing our risk management practices over time.

The ERM Framework documentation builds upon the findings of the maturity assessment presented to the Audits and Risk Management Committee in March 2023 and aligns with the 18-month maturity plan presented in November 2023. It supports our ongoing efforts to enhance the maturity of our risk management program and strengthen our resilience to emerging threats and uncertainties.

Key Changes

In reviewing the CalSTRS ERM Framework and aligning our practices with the maturity plan, staff has included some proposed changes. These changes include:

- Updating the ERM Framework graphic to better reflect our existing governance structure. (Page 7)
- Moving the semi-annual risk reporting, which currently includes the Risk Score Report, Heat Map, and Emerging Risk Universe Map from the full board to the Audits and Risk Management committee. This will provide the Audits and Risk Management committee with the opportunity to more closely evaluate and monitor enterprise risk reporting practices. The board will still receive reporting on emerging, existential and enterprise level risks that may impact strategic objectives. (Page 17)

¹ Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an organization dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the American Accounting Society, American Institute of CPAs, Financial Executives International, Institute of Management Accountants, and the Institute of Internal Auditors. [Applying the COSO ERM Framework](#)

Our goal is to continually improve risk and compliance reporting to the board and the Audits and Risk Management committee as the ERM program continues to mature.

This item is an Information item and staff intends to bring a subsequent Action item related to this framework at the September Audits and Risk Management Committee meeting. Staff however supports the Committee in approving this first reading, if so desired.

Strategic Plan Linkage: [Goal 1: Trusted stewards – Ensure a well-governed financially sound trust fund. \(FY 2022-25 Strategic Plan\).](#)

Board Policy Linkage: [Audits and Risk Management Committee Charter](#)

Optional Reference Material:

March 2023 ARM Committee, Item 7 – [Enterprise Risk Management and Compliance Services Framework and Maturity Recommendations](#)

November 2023 ARM Committee, Item 7 – [Enterprise Risk Management and Compliance Services 18-Month Maturity Plan.](#)