CALSTRS

Audits & Risk Management Committee

Item Number 4 – Open Session

Subject: Committee Education: Enterprise Risk Management Framework

Presenter(s): Julie Underwood / Lynn Bashaw

Item Type: Information

Date & Time: March 7, 2024 – 20 Minutes

Attachment(s): None

PowerPoint(s): ERM Framework Education

Item Purpose

The purpose of this item is to provide the Audits and Risk Management Committee with education about the CalSTRS Enterprise Risk Management (ERM) Framework. This will support the foundation for upcoming discussions and recommendations that will mature the enterprise risk management program.

Recommendation

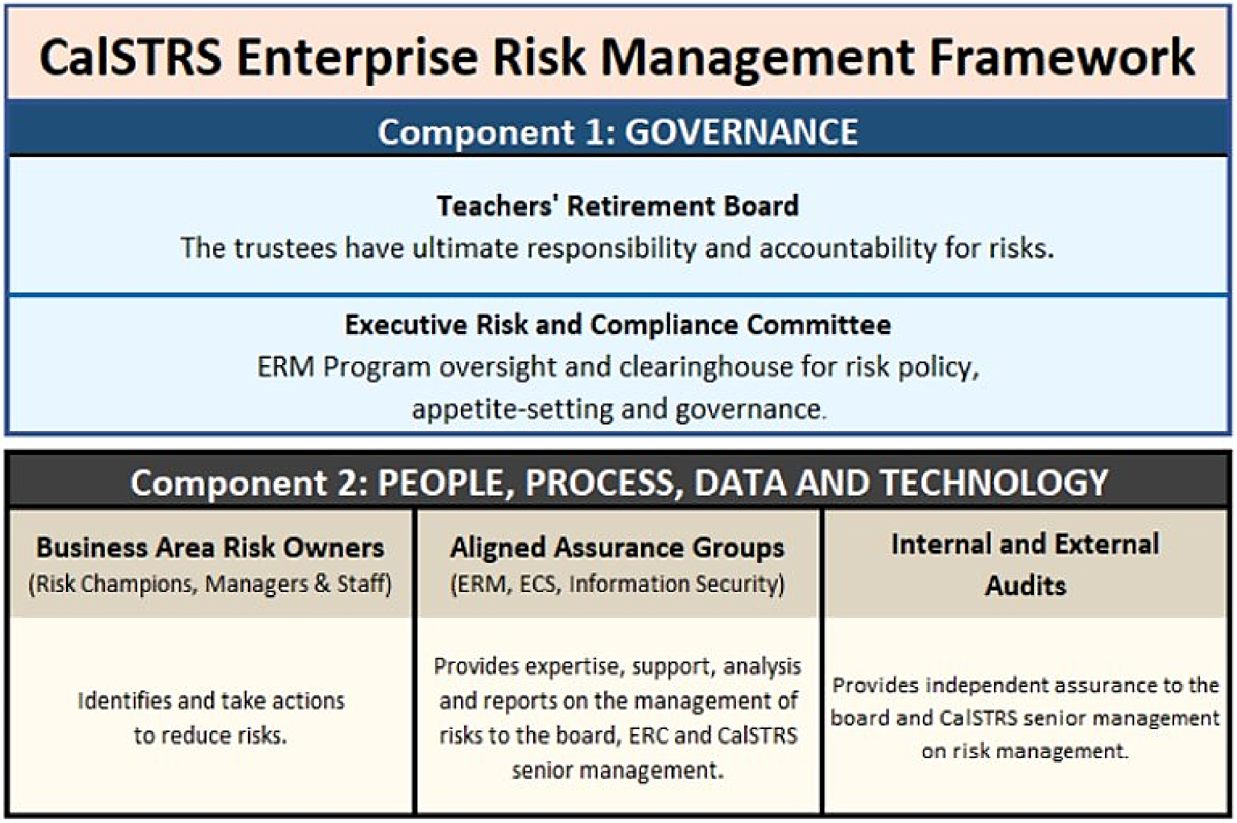
This is an information item only.

Executive Summary

A successful risk management program helps an organization consider the full range of risks it faces. Risk management also examines the relationship between different types of business risks and the cascading impact they could have on an organization's strategic goals. The purpose of the CalSTRS ERM Program is to successfully implement and sustain the CalSTRS ERM Framework, which is a set of policies, procedures, activities and tools used to effectively identify, assess and manage risks.

Figure 1, on the next page, shows the CalSTRS ERM Framework graphic that provides a high-level overview of how the various governing bodies and business areas within CalSTRS work together to manage risk.

Figure 1: CalSTRS ERM Framework



CalSTRS Enterprise Risk Management Framework

Component 1: GOVERNANCE

Teachers' Retirement Board
The trustees have ultimate responsibility and accountability for risks.

Executive Risk and Compliance Committee
ERM Program oversight and clearinghouse for risk policy, appetite-setting and governance.

Component 2: PEOPLE, PROCESS, DATA AND TECHNOLOGY

Business Area Risk Owners (Risk Champions, Managers & Staff)	**Aligned Assurance Groups** (ERM, ECS, Information Security)	**Internal and External Audits**
Identifies and take actions to reduce risks.	Provides expertise, support, analysis and reports on the management of risks to the board, ERC and CalSTRS senior management.	Provides independent assurance to the board and CalSTRS senior management on risk management.

The presentation will provide education on the current ERM Framework, which will support the foundation for upcoming discussions and recommendations to mature the enterprise risk management program, pursuant to Strategic Plan Goal 1, Objective E: Enhance how risks are defined, viewed and managed.

Background

Pursuant to the Board Governance Manual, Section 2, Item F: *Risk Management Policy*, CalSTRS considers risk management an essential component of strategic, operational, financial, and reputational management. CalSTRS faces a range of risks that can both positively (opportunities) and negatively (threats) impact the achievement of business objectives. The focus of CalSTRS risk management is the identification, assessment, and response to risks and the timely communication of the results of these processes. CalSTRS embeds risk management in all business practices to keep it relevant, effective, and efficient.

The board is responsible for:

1. Ensuring creation of a comprehensive approach and framework to anticipate, identify, analyze, prioritize, and manage key risks to the system's business objectives.
2. Providing the policy for an effective system of enterprise-wide risk management.

3. Establishing the overall enterprise risk appetite.
4. Approving management's strategy relating to key risks, including, but not limited to, strategic, operational, financial, compliance, reputational and investments.
5. Receiving reports on selected risk topics from time to time.
6. Ensuring risk assessments are performed periodically and completely.
7. Confirming board committees are overseeing the adoption of appropriate processes, methods, and tools for managing risks associated with business objectives in the committee's domain.
8. Communicating risk management activities and risk appetite established by the board.

The chief executive officer is responsible for:

1. Creating the risk governance structure, risk assessment and risk management practices, and the guidelines, policies, and processes for risk assessment and risk management based on the board policy and framework.
2. Ensuring management establishes a strategy relating to key risks, including, but not limited to, strategic, operational, financial, compliance, reputational and investments.
3. Instilling an awareness of risk and creating a responsibility for effective risk management at all levels within CalSTRS.
4. Establishing the methodology for measuring risk management performance.
5. Periodically conducting and reporting the results of risk assessments.

The ARM Committee performs a vital role in risk management by assisting the board to fulfill its fiduciary oversight responsibilities for the risk management framework. As outlined in the ARM Committee Charter, the board has delegated to the committee the responsibility, as it relates to risk management, to:

1. Review and recommend to the board changes, when necessary, to enterprise-wide risk management processes, governance, and related policies or infrastructure (framework).
2. Adhere to the Risk Management Policy established by the board.
3. Review emerging and significant risks specific to the area of responsibility of the committee, and reporting those risks to the board.

The Committee of Sponsoring Organizations (COSO)[1] publishes industry guidance on risk management framework principles and best practices. In 2017, COSO published updated guidance[2] that focused on integrating enterprise risk management with both strategy and

[1] The Committee of Sponsoring Organizations' (COSO) mission is to help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence. About Us | COSO

[2] COSO Enterprise Risk Management: Integrating with Strategy and Performance, published June 2017.

performance. In 2020, COSO released guidance[3] that emphasized harmonizing enterprise risk management with an organization's compliance and ethics programs.

In 2022, CalSTRS partnered with Weaver and Tidwell, LLP to assess our ERM program based on the COSO guidance and provided recommendations to mature the program. An 18-month maturity plan was presented to the ARM Committee in November 2023 which noted that the overall framework, including the charters, would need to be updated to fully support implementation of the maturity plan.

Next Steps

In support of the maturity plan, staff has worked to refine the framework graphic, fully document its components, and update supporting charter documents.

Evolution of the CalSTRS ERM Framework reflects our commitment to continuous improvement in managing risks effectively. By refreshing the framework graphic, staff aims to provide a visually intuitive representation of our risk management approach, enhancing clarity and alignment across the organization. Additionally, documenting the framework's components will provide education on key activities and processes, and continue to foster a culture of proactive risk management throughout the organization. Updating the charter documents will memorialize the integration of strategy and compliance into the framework and support the program's maturity.

At the May 2024 ARM Committee meeting, staff will present a first reading of the proposed updates to the risk management framework and its supporting charters, with an option for approval. A second reading will be scheduled for the September 2024 ARM Committee meeting, if needed.

Strategic Plan Linkage: Goal 1: Trusted stewards – Objective E: Enhance how risks are defined, viewed and managed.

Board Policy Linkage: Board Governance Manual, Section 2, Item F. Risk Management Policy.

Optional Reference Material: **November 2023 ARM Committee, Item 7 –** Enterprise Risk Management and Compliance Services 18-Month Maturity Plan**.**

[3] COSO Compliance Risk Management: Applying the COSO ERM Framework, published November 2020.