CALSTRS

Audits & Risk Management Committee

Item Number 7 – Open Session

Subject: Committee Education: Enterprise Risk Management & Compliance Services Framework and Maturity Recommendations

Presenter(s): Julie Underwood, Lynn Bashaw

Item Type: Information

Date & Time: March 1, 2023 – 30 minutes

Attachment(s): Maturity Assessment Executive Summary from Weaver

PowerPoint(s): Enterprise Risk Management & Compliance Services Framework and Maturity Recommendations

---

Item Purpose

The purpose of this item is to provide the Audits and Risk Management (ARM) Committee with education on CalSTRS Enterprise Risk Management Framework and provide the results of the Enterprise Risk Management and Compliance Maturity Assessment, in support of the CalSTRS Strategic Plan Goal 1, Objective E: Enhance how risks are defined, viewed and managed, and Goal 3, Objective D: Strengthen preparedness capabilities to address change and disruptions.

Recommendation

This is an information item only.

Executive Summary

In October 2022, CalSTRS engaged a consultant, Weaver and Tidwell LLP (Weaver), to conduct a maturity assessment of the Enterprise Risk Management (ERM) and Enterprise Compliance Services (ECS) programs. The goals of this assessment are to:

1) Evaluate the current state of the ERM and ECS programs;

2) Provide recommendations to align the framework and charters, and

3) Develop a roadmap to mature the programs based on industry best practices for risk management and compliance.

This report provides the committee with education on the current framework of the ERM and ECS programs, a summary of the recommendations made by Weaver to further mature the ERM and ECS programs, and management's next steps for completing a plan to mature both programs. For more detailed information on the maturity assessment results, see Attachment 1.

Background

CalSTRS ERM FRAMEWORK

Figure 1 shows the CalSTRS Enterprise Risk Management Framework, which provides a visual overview of where ERM and ECS are situated as part of the aligned assurance groups in the second line of defense under Component 2: People, Process, Data and Technology. As noted in the framework, ERM and ECS provide expertise, support, analysis, and reporting on the management of risks to the board, various committees, and senior management.

Figure 1: CalSTRS ERM Framework

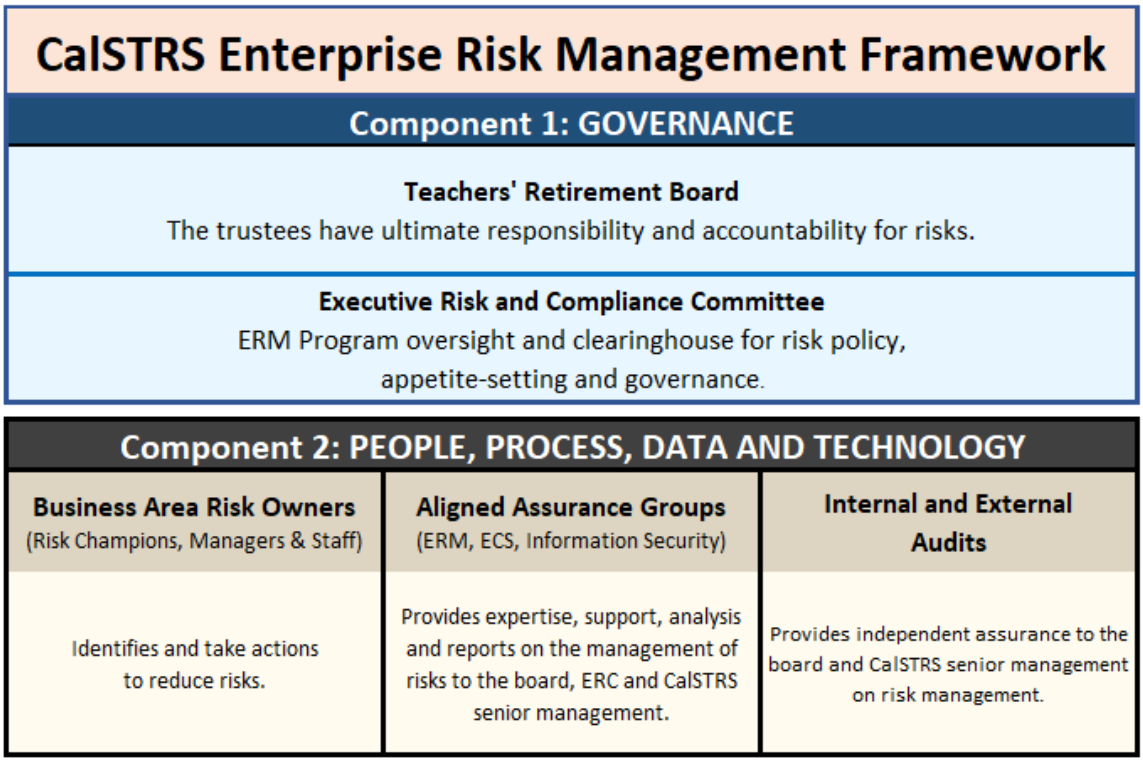


Figure 2, on the next page, provides more detail on the oversight, implementation, and reporting responsibilities for the entities described in the ERM Framework. This figure is intended as a high-level overview and does not include all of CalSTRS' risk and compliance efforts. Risk and compliance efforts require the collective effort and support of all CalSTRS employees.

Figure 2: ERM Framework Responsibilities and Reporting Matrix

CalSTRS ERM Framework: Responsibilities and Reporting Matrix			
Component	**Entity**	**Risk and Compliance Responsibilities**	**Reports Received**
Component 1: GOVERNANCE	Teachers' Retirement Board	•Primary responsibility for Enterprise-Wide Risk Oversight •Approves Risk Management Policy	•ERM Semi-Annual Risk Report •Emerging/Existential Risk Report •Information Security Reports •State Leadership Accountability Act (SLAA) Reporting •Review of Funding Levels & Risks Report
	Audits and Risk Management (ARM) Committee	•Oversight of ERM Framework •Oversight of Financial Risk Reporting •Oversees design and implementation of Compliance Program •Oversight of Internal/external audits	•ECS Annual Compliance Plan/Plan Updates •Periodic reports on Allegations of Suspected Misconduct •Annual Audit Plan/Audit Reports •External Audit of Financial Statements
	Investment Committee	•Oversight of investment risks including Investment Policy Framework	•Investment Compliance Report •Portfolio Risk Reports
	Executive Risk and Compliance Committee (ERCC*)	•Implements Board policies and ERM Framework •Provides ongoing guidance and support to the ERM and ECS teams •Approves the ERM and ECS programs and ERCC Charter	•ERM Quarterly Risk Matrix Update •ECS Quarterly Compliance Reporting •Annual ERM Team & RCN Workplans •Emerging/Existential Risk Reports •Results of Annual Branch Risk Assessment
Component	**Entity**	**Risk and Compliance Responsibilities**	**Reports Generated**
Component 2: PEOPLE, PROCESS, DATA, and TECHNOLOGY	Risk Champion Network (RCN)/Managers & Staff	•RCN is comprised of representatives from the various branches •RCN's collaborate with ERM to identify, monitor, and report on quarterly risk indicators for their respective branches	•RCN Annual Workplan •ERM Quarterly Risk Matrix Update •Annual Branch Risk Assessment •Review of Funding Levels & Risks Report
	Enterprise Risk Management (ERM)	•Implement and sustain the CalSTRS ERM Framework, which is a set of policies, procedures, activities, and tools used to manage risks	•ERM Semi-Annual Risk Report •Emerging/Existential Risk Report •State Leadership Accountability Act (SLAA) Reporting •Annual ERM Team Workplan
	Enterprise Compliance Services (ECS)	•Promote and enhance a culture of ethics and compliance to respond to potential violations of law, regulations, and policies through collaboration and coordination	•ECS Annual Compliance Plan and Plan Updates •ECS Quarterly Compliance Reporting •Periodic reports on Allegations of Suspected Misconduct
	Information Security Office (ISO)	•Protects CalSTRS data assets from unauthorized access or use	•Information Security Reports
	Audit Services (Internal & External Audits)	•Provide independent, objective assurance through internal and external audit and consulting services	•Annual Risk Assessment/Audit Plan •Audit Reports •External Audit of Financial Statements

**At the December 2022 meeting, the ERC formally changed its name to the ERCC to recognize the inclusion of compliance reporting to this committee.*

COMPONENT 1: GOVERNANCE

This section provides a brief overview of the Governance component identified in the CalSTRS Enterprise Risk Management Framework.

Teachers' Retirement Board

The board's governance manual includes a Risk Management Policy that states, in part:

> CalSTRS considers risk management an essential component of strategic, operational, financial, and reputational management. 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. In keeping with this approach, the board shall have the primary responsibility for CalSTRS enterprise-wide risk oversight, while board committees are chartered with oversight of specific areas of risks.

The policy also delegates to the chief executive officer the responsibility to create 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.

Audits & Risk Management (ARM) Committee (Board Committee)

The ARM Committee performs a vital role in the organization by assisting the board to fulfill its fiduciary oversight responsibilities, including the CalSTRS Risk Management Framework. The ARM Committee's charter provides enterprise risk and compliance responsibilities as follows:

- Reviewing and recommending to the board changes, when necessary, to enterprise-wide risk management processes, governance, and related policies or infrastructure (framework).
- Adhering to the Risk Management Policy established by the board.
- Reviewing emerging and significant risks specific to the area of responsibility of the committee, and reporting those risks to the board.
- Overseeing the design and implementation of the Compliance Program, including the policies and procedures to help prevent and detect violations of law and to promote business ethics.
- Reviewing the effectiveness of the system for monitoring compliance with applicable laws, regulations and policies.
- Reviewing the annual compliance plan and receiving periodic progress reports.
- Overseeing CalSTRS' policies and procedures for the receipt and handling of allegations of suspected misconduct and receiving reports on a periodic and as-needed basis regarding significant reports received.

Investment Committee (Board Committee)

The CalSTRS investment portfolio is invested to maximize return at a prudent level of risk. The Investment Committee was established by the Teachers' Retirement Board to oversee all matters relating to these investments. The committee is charged to oversee the system's assets for the exclusive purpose of providing benefits to the participants and their beneficiaries and to maximize the financial stability of the system in an efficient and cost-effective manner. The committee members carry out their duties with the care, skill, prudence, and diligence of a prudent person acting in a similar institutional investment board member capacity, and strive to follow sound policies and procedures that enhance informed, fair, and open decision making. The Investment Committee's responsibilities as it relates to risk and compliance include:

- Determining the system's overall investment objectives for the various plans, risk tolerance and performance standards in accordance with the California Constitution and the Teachers' Retirement Law.
- Determining the asset allocation of the State Teachers' Retirement Plan, including consideration of asset classes and sub-classes not currently utilized.
- Determining the overall State Teachers' Retirement Plan Investment Policy and Management Plan as well as asset class allocation, setting risk budgets, and program investment policies.
- Monitoring the compliance of CalSTRS investments with applicable investment policies and investment resolution, including those regarding environmental, social and governance risks and the system's investment policies.
- Reviewing emerging and significant risks specific to the area of responsibility of the Committee and report those risks to the board.
- Determining and ensuring compliance with the appropriate reporting standards and time horizons.

Executive Risk and Compliance Committee (ERCC) (Staff Committee)

The purpose of the Executive Risk and Compliance Committee (ERCC) is to provide oversight of the CalSTRS Enterprise Risk Management (ERM) Program and the Enterprise Compliance Services (ECS) Program.

The ERCC consists of the following members: Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, Chief Investment Officer, Chief Technology Officer, Chief Benefits Officer, General Counsel, Chief Administrative Officer, Chief Public Affairs Officer, Deputy Chief Investment Officer and System Actuary. In addition, the following CalSTRS staff serve in a consultative role to the ERCC: the ERM Team, Chief Auditor, Communications Director, Director of Enterprise Risk Management & Compliance Services, Human Resources Director, Enterprise Strategy Director and Information Security Officer.

The primary responsibilities of the ERCC include:

- Provide leadership and commitment to risk and compliance management by establishing a sound risk and compliance awareness culture throughout CalSTRS.
- Provide ongoing guidance and support to the ERM and ECS teams for the administration of the ERM and ECS frameworks and programs.
- Ensure the accurate, timely and consistent flow of risk and compliance management information to the board and ARM committee including reports on ERM and ECS Program's risk and compliance activities on a semi-annual basis.
- Approve the ERM and ECS Programs and ERCC Charter.
- Determine enterprise-wide key risks.
- Identify emerging and existential risks that threaten achievement of business goals and strategies and deploy resources as necessary to manage emerging risks.
- Identify and resolve weaknesses or gaps in risk mitigations.
- Manage risks through the assignment of risk owners and deployment of resources.
- Provide oversight of risk champion activities, approve the RCN's Charter, RCN's Annual Work Plan and receive reports twice a year on the RCN's Annual Work Plan progress.
- Review and approve the ERM and ECS Team's Annual Work Plans and receive reports twice a year on the ERM and ECS Team's Annual Work Plan progress.
- Approve ERM and ECS related policies developed by either the ERM or ECS Teams in collaboration with the RCN.
- Review the effectiveness of the ERM and ECS Programs annually and review ERM and ECS policies and charters biennially.

COMPONENT 2: PEOPLE, PROCESS, DATA, and TECHNOLOGY

This section provides a brief overview of the People, Process, Data, and Technology component identified in the CalSTRS Enterprise Risk Management Framework.

Risk Champion Network (RCN)/Managers & Staff

Managers and staff throughout the organization are responsible for various risk and compliance activities. This includes, but is not limited to, risk awareness, supervisory review, quality assurance, and compliance with policies and procedures.

In addition, the RCN is comprised of individuals selected by each branch executive based on specific selection criteria. Nine risk champions represent the following branches: Executive, Public Affairs, Investments, Technology Services, Benefits & Services, General Counsel, Administrative Services, Financial Services and Actuarial Resources (a subset of the Financial Services branch).

Risk champions meet regularly with the ERM and ECS teams, their branch executive, senior leadership, and alternate risk champion and between and among their branch managers.

The primary responsibilities of the RCN include:

- Biennially review the RCN Charter and provide recommendations to the ERC for any revisions.
- Develop and implement an annual RCN Work Plan.
- Collaborate with the ERM and ECS Teams to provide reports twice a year to the ERC on the RCN's Annual Work Plan progress.
- Identify, monitor and report risk indicators on a quarterly basis.
- Manage and organize the risk information and mitigation efforts within the risk champions' respective branch.
- Maintain communications through the regular meetings and the established reporting documents to openly discuss and report potential emerging or escalated risks with the ERM and ECS teams.
- Assist in incorporating and supporting a strong risk and compliance awareness culture into the risk champions' respective branch.
- Provide input and feedback on the ERM training courses.
- Participate in the annual review of the ERM Program including the review of ERM policies.
- Collaborate with respective branch executive and branch leadership to review and update the inherent and residual risk scores which are reported to the board semi-annually.

Enterprise Risk Management (ERM)

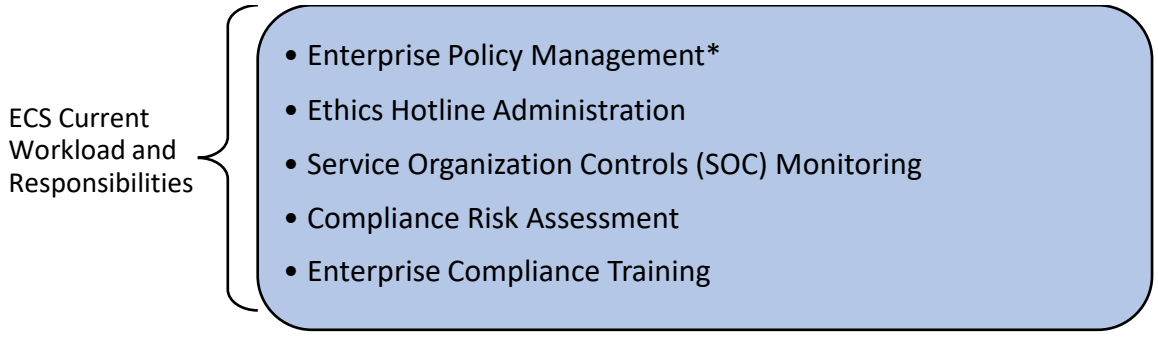
Enterprise risk management (ERM) is a program that CalSTRS leadership uses to identify, assess and prepare for any risks that may interfere with CalSTRS operations and objectives. The purpose of the ERM Program is to successfully implement and sustain the CalSTRS ERM Framework, which is a combination of oversight bodies, policies, procedures, activities and tools used to manage risks. The ERM Program also provides oversight in achieving CalSTRS ERM vision, which is to maximize CalSTRS' ability to achieve its strategic and business objectives. Figure 3, on the next page, highlights the primary responsiblities ERM currently manages.

Figure 3: ERM Current Responsibilities

Enterprise Compliance Services (ECS)

Effective compliance risk management requires a reporting and review structure that ensures compliance risks are effectively identified and assessed, and that appropriate controls and responses are in place. ECS staff works with the various business areas and the RCN to identify and coordinate processes to ensure compliance with laws, regulations, standards, and applicable policies in the achievement of strategic goals and objectives. ECS helps to support a strong culture of ethics and compliance. Figure 4 highlights the current responsibilities that ECS manages.

Figure 4: ECS Current Responsibilities



**Excluding investment and board policies.*

Information Security Office (ISO)

The Information Security Office (ISO) is CalSTRS' authority on information security and cybersecurity matters. The Information Security Office protects CalSTRS data assets from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. ISO provides the board with regular security updates during closed sessions.

Audit Services

Audit Services provides independent, objective assurance and consulting services designed to add value and improve CalSTRS operations. Audit Services assists CalSTRS in accomplishing its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes. Audit Services provides a wide range of quality, independent internal auditing assurance and consulting services for the ARM Committee and CalSTRS management.

MATURITY ASSESSMENT RESULTS

The purpose of the maturity assessment, conducted by Weaver, is to show the current levels of maturity for the ERM and ECS programs. It also helps to inform the roadmap to the future state, on both a short- and long-term basis. It should be expected that moving from each level of maturity includes a cost and complexity component as well as more advanced business practices for the organization.

Weaver evaluated the maturity of the Enterprise Risk Management (ERM) and Enterprise Compliance Services (ECS) functions for CalSTRS using a methodology modeled after the two industry standards used to help establish each of the teams, the COSO Enterprise Risk Management and Society of Corporate Compliance and Ethics (SCCE) frameworks. For more information on the maturity assessment process and the results, see Attachment 1.

Overall, Weaver found that CalSTRS has a well-established framework for governance of the ERM Program, with all levels of management across the organization involved in key activities. This provides consistency of reporting, communication, and implementation of the risk management methodology across the organization. Weaver also noted that the Risk Champion Network (RCN) has significant involvement from all levels of management across the organization and is well supported by executive leadership.

Weaver also found that ECS has been successful in marketing the Ethics Hotline and partners with Communications, Legal and Human Resources on Code of Ethics communications.

The maturity assessment conducted by Weaver identified four *primary themes* that, if addressed will help to accelerate the maturity of the ERM and ECS programs. The four themes are as follows:

1. Risk Appetite and Risk Tolerance
2. Compliance Access and Authority
3. Advanced ERM Integration
4. Resources (People, Process, and Technology)

Weaver's *recommendations* included 8 items for ERM and 11 items for ECS.

ERM Maturity Recommendations

1. Define and Implement Risk Appetite and Risk Tolerance
2. Prioritize Risks and Develop Key Risk Indicators (KRIs)
3. Apply Structured Approach to Risk Response
4. Obtain Access to Data and Systems for ERM
5. Define Metrics to Drive Execution and Integration
6. Utilize Existing Tools to Perform Analytics
7. Automate Risk Data Collection and Reporting
8. Implement ERM-specific Professional Development Program

ECS Maturity Recommendations

1. Determine ECS Role in a Distributed Compliance Model
2. Provide Oversight, Monitoring, Testing, and/or Ownership of Conflicts of Interest
3. Build Standardized Oversight and Approach to Distributed Compliance Functions
4. Access to Branch Systems and Data
5. Establish Ownership of Compliance-related Policies
6. Oversee Policy and Regulatory Implementation
7. Participate with Investigations in Ethics and Compliance Concerns
8. Consult on Enforcement for Compliance Issues
9. Develop Annual Compliance Training Program
10. Implement Compliance-specific Professional Development Program
11. Obtain Resources for Expanded Roles

Weaver noted that the overall framework, including the charters for ERM, ECS, ERCC, and RCN will need to be updated to fully support the implementation of these recommendations. For additional information on the maturity assessment process and maturity levels, Weaver's executive summary report is provided as Attachment 1.

NEXT STEPS

The position of Director of ERM and ECS was recently established, recruited for, and filled. The new director will evaluate the proposed recommendations from Weaver's maturity assessment and, in collaboration with senior management, develop a maturity roadmap plan that will be presented to the ARM Committee in November 2023.

Strategic Plan Linkage: Goal 1: Trusted Stewards, Objective E: Enhance how risks are defined, viewed and managed, and Goal 3: Sustainable Organization, Objective D: Strengthen preparedness capabilities to address change and disruptions.

Board Policy Linkage: ARM Committee Charter