CALSTRS

Audits & Risk Management Committee

Item Number 7 – Open Session

Subject: 2022 Enterprise Compliance Services Plan

Presenter(s): Cheryl Cervantes-Dietz

Item Type: Information

Date & Time: November 4, 2021 – 15 minutes

Attachment(s): Attachment 1 - 2022 Enterprise Compliance Services Plan

PowerPoint(s): PowerPoint 1 –2022 Risk-Based Enterprise Compliance Services Plan

---

PURPOSE

The purpose of this item is to provide the Audits and Risk Management (ARM) Committee with the 2022 Enterprise Compliance Services' Plan. This Plan was developed through an integrated risk assessment process that set the priorities for the Enterprise Compliance Services program in the 2022 calendar year.

DISCUSSION/SUMMARY

2021 Compliance Plan Update

Enterprise Compliance Services (ECS) continues to make progress on key priorities within the Plan. Below are a few highlights of the progress made since the last update to the Committee.

- ✓ Published CalSTRS External Compliance Reporting Matrix on ECS SharePoint
- ✓ In partnership with Communications finalized the revision of CalSTRS Code of Ethics and Business Conduct.
- ✓ Developed a Policy Review Checklist that addresses and ensures policies are in the prescribed format, have relevant and clear content and includes integrated business reviews, if necessary.
- ✓ Partnered with Ombuds and Human Resources to expand the use of the Compliance & Ethics Hotline case management system.
- ✓ Increased compliance collaboration and awareness through engagement with Compliance Advisory Committee members.
- ✓ Developed two user guides to assist in the administration and management of hotline cases.

- ✓ Executed an integrated assurance risk assessment process.
- ✓ Continued coordination of System and Organization Controls report reviews submitted by third-party vendors providing services to CalSTRS.
- ✓ Enhanced compliance risk taxonomy to further reflect CalSTRS compliance risks.
- ✓ Initiated development of the following:
  - Organization-wide Compliance Accountability Matrix
  - Mandated Training Matrix
  - Procurement Processes, Legal Requirements, and Controls Library

Compliance Framework:

ECS coordinates across the organization to support CalSTRS in meeting its compliance and ethical responsibilities reinforced by the framework outlined in the 2022 Enterprise Compliance Services Plan, Attachment 1. This framework aligns with key regulatory requirements, guiding frameworks, and other leading practices. A key element of the overall Compliance Framework is performing a Compliance Risk Assessment, discussed below, to identify and understand the areas of greatest compliance risk to the organization.

Compliance Risk Assessment

In collaboration with Internal Audits and Enterprise Risk Management, ECS performed an organizational compliance risk assessment. The compliance risk assessment allows ECS to prioritize and focus its resources towards CalSTRS most significant compliance and ethical risks. The figure below illustrates the approach used to assess compliance risks.

Figure 1: ECS Risk Assessment and Plan Development Process

Based on the results of the organization compliance risk assessment, ECS will focus its compliance efforts as outlined in the 2022 Enterprise Compliance Services Plan, see Attachment 1.

2022 Enterprise Compliance Services' Plan

Professional Standards

As recommended by the United States Federal Sentencing Guidelines, and the Society for Corporate Compliance and Ethics (SCCE), CalSTRS Enterprise Compliance Services (ECS) presents the *2022 Enterprise Compliance Services Plan* (Plan) to the Audits and Risk Management (ARM) Committee.

Enterprise Compliance Services Mission

The mission of ECS is to support the organization in fostering and maintaining a strong ethical and compliant culture. To achieve our mission, ECS will:

- Raise awareness on CalSTRS compliance obligations with applicable laws, regulations, policies, and standards, and promote acceptable ethical behaviors
- Assist with the identification, mitigation, and monitoring of CalSTRS compliance risks
- Communicate and educate on enterprise compliance-related topics
- Act as a resource to the organization in ensuring CalSTRS complies with applicable laws, regulations, policies, and standards

ECS Organization and Charter

ECS serves as a second line of defense function within the CalSTRS risk management framework, responsible for overseeing an enterprise-wide compliance program and monitoring of risks for non-compliance with applicable law and regulations.

The ECS Charter defines reporting relationships, program objectives, roles, and responsibilities of the ECS staff.

- The ECS Director reports to a level within the organization that allows ECS to fulfill its responsibilities.
- The ECS Director has access to the ARM committee and provides reports on the status of the Compliance program.
- The ARM committee oversees development of the annual Plan and reviews for any potential for impairment to objectivity with Audit Services.

Professional Organizations

ECS staff hold memberships in several professional organizations. These organizations serve as excellent sources of information and provides ECS staff with access to compliance best practices, industry standards, business management and other professional compliance topics.

Certifications

ECS staff are expected to attend training provided by the SCCE and obtain certification as a Certified Compliance and Ethics Professional (CCEP). Annually, ECS staff must obtain at least 20 hours of compliance-related continuing education to maintain the CCEP certification. Because of the pandemic and travel restrictions, ECS staff have not been able to obtain the training necessary to obtain CCEP certification.

Plan Progress

Interim changes to the Plan may occur due to changes in business risks, timing of CalSTRS' initiatives, and resource availability. ECS will report Plan progress and changes to Executive management and to the ARM committee.

Compliance Plan Scope and Development

This Plan covers the calendar year period from January 1, 2022 through December 31, 2022 and is designed to continue developing the Enterprise Compliance program, given the existing staff and approved budget. ECS completed a Compliance Risk Assessment which guides the development of this Plan using a framework to prevent, detect, and respond to instances of ethical misconduct or failing to meet our legal, regulatory, or policy compliance obligations. Below is ECS 2022 Compliance Plan:

1.0 Governance: *Structure the program with clearly defined roles & responsibilities*

- Facilitate Compliance Advisory Committee Meetings to Address Compliance Initiatives
- Publish Compliance and Ethics Accountability Matrix
- Continue Partnership Meetings with Internal Stakeholders
- Publish Enterprise Training Requirements Matrix
- Review and Update Enterprise Compliance Services Charter

2.0 Culture: *Ethical & compliant behavior embedded in the foundation & daily operations*

- Develop Activity-Based Learning and Communication for CalSTRS Revised Code of Ethics and Business Conduct
- Onboard Compliance Partners to ECS Regulatory Tracking Subscription for Increased Understanding of Compliance Obligations
- Develop Ethical Decision Making and Reporting Learning Aids to Promote Culture of Ethics
- Develop Communication Guides for Leaders to Address Specific Compliance Obligations as Relates to Business Processes

3.0 Risk Assessment: *Periodic assessments of risk exposure related to misconduct or non-compliance with laws, regulations, policies, & standards*

- Continue to Socialize and Update Compliance Risk Taxonomy
- Refine Compliance Risk Scoring Criteria
- Perform Iterative Compliance Risk Assessments and Update Compliance Initiatives as Needed
- Participate in the Implementation of the Governance, Risk and Compliance Tool

4.0 Policies & Standards: *Defined guidance to support organizational ethical expectations & compliance with applicable laws and regulations*

- Continue Coordination of Annual Policy and Biennial Standard Reviews
- Develop and Distribute Policy Management Handbook
- Update Policy Mapping to Legal Requirements Library
- Identify Policies Related to Highest Compliance Risks
- Implement Knowledge-Based Challenge into Annual Policy Attestation Process

5.0 Training & Communication: *Appropriately tailor subject matter topics to support understanding of compliance & ethics*

- Continue to Communicate and Promote through CalSTRS Intranet (Central), Roadshows, Newsletters, and ECS SharePoint on Below Topics:
  - Revised Code of Ethics and Business Conduct
  - Compliance Accountability Matrix (Compliance Roles & Responsibilities)
  - Enterprise Training Matrix
  - Regulatory Changes
  - Policy Highlights (Focus on Highest Ranked Compliance Risks)
  - Compliance & Ethics Hotline
- Expand Existing Training to Include Compliance and Ethical Topics
- Deliver Communication Aids or Training on Below Topics:
  - Regulatory Requirements Specific to Business Area Processes
  - Policy Requirements Specific to Business Areas
  - Compliance & Ethics in a Blended Work Environment
  - Case Management Responsibilities
- Update Communication Plan as Needed
- Promote Compliance and Ethics Awareness Week

6.0 Confidential Reporting: ***Efficient & effective mechanism that allows anonymous reporting of compliance & ethical concerns***

- In Collaboration with Public Affairs, Communicate/Educate External Stakeholders on Reporting Mechanisms
- Continue to Assess and Promote Importance of Speaking Up
- Distribute Compliance and Ethics Hotline Reporting Cards
- Identify Trends & Recommend Potential Mitigations

7.0 Case Management & Response: ***System & processes to efficiently and effectively manage, investigate & resolve hotline reports***

- Identify Case Management Process Improvements through Data Analytics
- Continue to Assess Compliance & Ethics Reporting Trends for Remediation
- Identify Opportunities for Expanded Use of Case Management System

8.0 Monitoring: ***System for routine monitoring of organizational compliance risk, controls & behaviors***

- Identify Opportunities to Embed Controls into Procurement and Human Resource Compliance Processes
- Partner with Procurement on Contract Management Compliance
- Collaborate with Facilities Management to Document its Processes, Legal Requirements and Controls
- Update and Validate External Compliance Reporting Matrix
- Coordinate with Compliance Assurance Partners on Risk Mitigation Roles & Reporting
- Assist Internal Stakeholders on Resolution of Outstanding Audit Issues

9.0 Third Party Compliance Management: ***Risk-based application of due diligence over third-party relationships***

- Develop Third-Party/Supplier Code of Conduct
- Assist Procurement in the Development of Contract Manager Monitoring Tools, Communications, and Training
- Collaborate with General Counsel on Third Party Risk Management
- Coordinate Third-Party System and Organization Controls (SOC) Reporting Review Process
- Continue to Refine SOC Report Review Process

10.0 Program Management: ***Defined structure to manage, measure & evaluate program effectiveness***

- Work with Enterprise Strategy Management to Develop Compliance & Ethics Survey
- Publish ECS Compliance and Ethics Accomplishment Report
- Perform Maturity Assessment of Compliance Program