



Enterprise Compliance Services Program Charter

Approved: Month XX, 2024

Introduction

CalSTRS is committed to maintaining a robust enterprise risk management framework that enhances decision-making, protects assets, and ensures compliance with regulatory requirements. The Enterprise Compliance Services (ECS) Program supports the enterprise risk management framework by promoting compliance with organizational policies, ethical standards, and regulatory requirements.

The ECS Program plays a pivotal role in our organization's strategic governance by working with management in identifying, assessing, and managing compliance risks that could impact our objectives. This charter serves as a guiding document governing the ECS Program and is an essential component of the overall Enterprise Risk Management Framework.

Purpose

The primary purpose of this charter is to document the formalized program for managing compliance risks across the organization. It aims to define the scope and responsibilities necessary for the effective implementation of the ECS Program. Furthermore, it underscores the commitment to ensure alignment with organizational objectives and strategy. This includes supporting the board's Risk Management Policy¹ and the Chief Executive Officer's responsibilities delegated therein.

Composition

The ECS Program is administered by a dedicated team within the Financial Services Branch with sufficient knowledge and expertise to support the program. Under the general direction of the Chief Financial Officer (CFO), the Director of Enterprise Risk Management and Compliance Services leads the ECS team.

Scope

The ECS Program supports all business areas in identifying, evaluating, monitoring, and mitigating risks of noncompliance with applicable laws, regulations, and CalSTRS policies. However, two areas of compliance are managed by other business areas. Conflict of interest reporting is administered by the Office of Legal Ethics and Accountability, and compliance and ethics activities related to the Investments Branch are managed by Investment Compliance. ECS will continue to be a resource for these business areas and support their compliance efforts, as needed.

Responsibilities

ECS Program responsibilities include:

- **Risk assessment:** Conducting regular compliance risk assessments to support identification, evaluation, and mitigation of potential compliance risks across the organization.

¹ [Board Governance Manual, Section G: Risk Management Policy](#)

- **Policy administration:** Administering and communicating organizational policies in collaboration with relevant stakeholders to ensure compliance with laws, regulations, and management direction.
- **Code of Ethics and Business Conduct:** Establishing and reinforcing a Code of Ethics and Business Conduct to guide the behavior of employees in alignment with organizational values.
- **Training and awareness:** Providing training and awareness programs to ensure all employees understand their roles and responsibilities in managing compliance risks within their respective areas.
- **Monitoring and reporting:** Implementing monitoring mechanisms to detect and prevent deviations from established policies and providing regular reports to the Audits and Risk Management committee and CalSTRS management. This could include ad hoc reporting to the board or another board committee, as requested.
- **Third-party risk management:** Assisting the organization with assessing and mitigating compliance risks associated with third parties. This includes administration of the SOC² reporting process and supporting third-party procurement compliance.
- **Hotline administration:** Managing a confidential and anonymous hotline for employees to report concerns or potential violations related to compliance and ethics.
- **Integration:** Integrating compliance risk management into strategic planning, decision-making processes, and day-to-day operations throughout the organization.

Access

To fulfill the mission and objectives of the ECS program, the ECS Program will have full and unrestricted access to all CalSTRS functions, records, files and information systems, personnel, contractors, physical properties, and any other items relevant to performing compliance risk assessment and evaluating compliance risk mitigations. Due to the sensitive and non-public nature of investment data, ECS staff will not access investment data. ECS staff will protect the information acquired in the course of their duties. Staff will not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of CalSTRS or to the ECS Program

Program Self-Evaluation

The ECS Program shall conduct periodic self-evaluations to assess the effectiveness of its processes, controls, and overall performance. These evaluations will include reviews of risk management policies, procedures, and methodologies, as well as feedback from stakeholders. Any identified areas for improvement shall be addressed promptly to enhance the efficiency and effectiveness of the ECS Program.

² System and Organization Controls (SOC) reports are issued by independent Certified Public Accountant (CPA) and are designed to assist with providing assurance over control effectiveness of third-party service providers.

Revisions

This charter shall be reviewed and revised every other year, or as necessary, to ensure its alignment with the organization's objectives, evolving risk landscape, and regulatory requirements. Any proposed revisions to the Charter shall be presented to the Audits and Risk Management committee for approval.

Approved by Audits and Risk Management Committee: Month XX, 2024