CALSTRS

Audits & Risk Management Committee

Item Number 7 – Open Session

Subject: Enterprise Risk Management and Compliance Services 18-Month Maturity Plan

Presenter(s): Julie Underwood and Lynn Bashaw

Item Type: Information

Date & Time: November 2, 2023 – 15 minutes

Attachment(s): Enterprise Risk Management and Compliance Services 18-Month Maturity Plan

PowerPoint(s): 18-Month Maturity Plan Presentation

Item Purpose

The purpose of this item is to provide the Audits and Risk Management (ARM) Committee with the proposed Enterprise Risk Management and Compliance Services 18-Month Maturity Plan, 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. This strategic initiative is designed to enhance CalSTRS' ability to identify, assess, and mitigate risks while ensuring an ethical culture and compliance with relevant regulations.

Recommendation

This is an information item only.

Executive Summary

In today's rapidly evolving business landscape, effective risk management and compliance are paramount for organizations to thrive and to safeguard their reputation. This report outlines 18-month plans that work towards maturing the Enterprise Risk Management (ERM) program and the Enterprise Compliance Services (ECS) programs in alignment with industry standards.

A maturity assessment was performed by Weaver and Tidwell, LLP (Weaver) that was presented to the ARM Committee in March 2023. This assessment included several recommendations for maturing the ERM and ECS programs.

In developing the 18-month maturity plan, the ERM and ECS teams evaluated Weaver's recommendations for the following:

- Ease of implementation
- Overall practicality
- Order of implementation
- Impact to other business areas
- Resource requirements
- Timing

Many of the recommendations included in this initial 18-month plan are designed to build or enhance our internal ERM and ECS infrastructure. Recommendations requiring significant support from other business areas or more internal staffing resources, will be included in future workplans. Some recommendations were not selected for implementation but may be reevaluated later.

Overall, this maturity plan includes deployment of enterprise risk software, an update to the enterprise risk framework, updates to the ERM and ECS charters, staff training, third-party risk management program support, integration of risk appetite statements, and implementation of key risk indicators. The maturity plan also includes developing an ECS procedure manual, mapping the compliance activities across the organization, and outlining the framework for a compliance monitoring program.

This maturity plan was developed by the ERM and ECS staff and presented to the Executive Risk and Compliance Committee (ERCC), the Risk Champion Network (RCN) and various stakeholders to solicit feedback, answer questions, and share our enthusiasm for elevating the risk and compliance culture at CalSTRS. We are pleased to provide you with a plan we feel is realistic and achievable given our current level of maturity and our internal resources.

This plan is expected to cover the period of January 1, 2024, through June 30, 2025. As we mature the programs we will regularly assess and report on our progress and challenges to the ERCC and to the ARM Committee. Towards the end of this 18-month plan, we will develop another workplan that continues the progress towards our maturity goals.

Our vision is to transform our risk and compliance programs into best-in-class models, meeting or exceeding industry standards. This maturity project will enable us to proactively identify and address risks, further strengthen our resilience in the face of challenges, and maintain a culture of compliance and ethical behavior.

Background

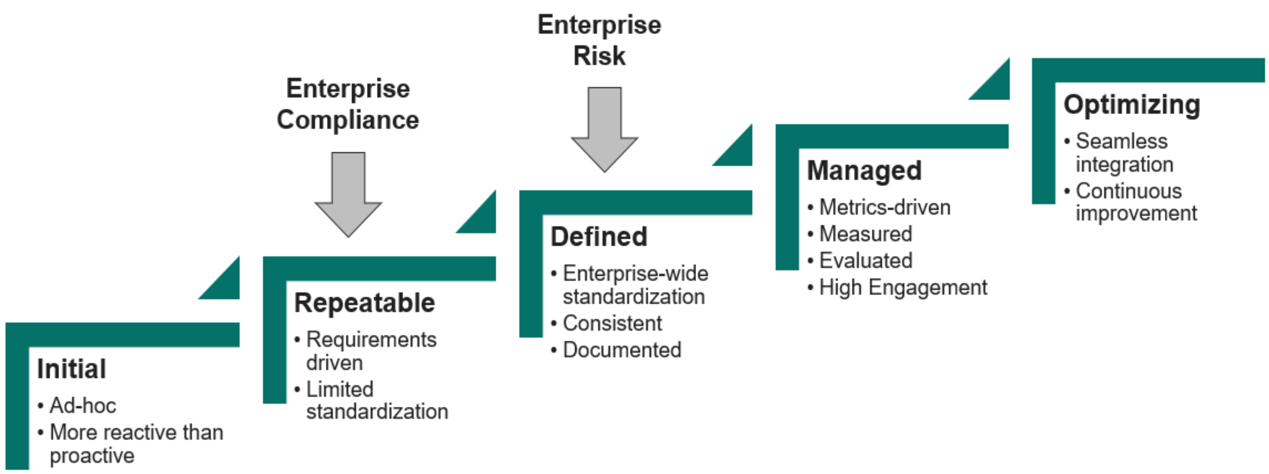
In October 2022, CalSTRS engaged a consultant, Weaver and Tidwell LLP (Weaver), to conduct a maturity assessment of the Enterprise Risk Management (ERM) and Enterprise Compliance Services (ECS) programs.

The goals of the maturity assessment were 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.

Weaver evaluated the ERM and ECS program maturity 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. Figure 1 shows the current maturity level of the Enterprise Risk Management and Compliance Services programs based on these models.

Figure 1: Current maturity level of the enterprise risk program and enterprise compliance program



In March 2023, the recommendations were presented to the ARM Committee. 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'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, would also need to be updated to fully support the implementation of these recommendations.

It is important to note that it could take several years to mature the ERM and ECS programs to their desired state. Moving towards higher levels of maturity also comes with increased complexity and the need for communication and buy-in across the organization. In addition, it may not be desirable to mature both the ERM and ECS programs to the optimized state because of the cost and complexity involved.

Maturity Plan

In consideration of Weaver's assessment, along with internal discussions with senior leaders, an 18-month plan was developed that will guide ERM and ECS' progress toward maturity through the period of January 1, 2024 through June 30, 2025. As the ERM and ECS programs have a different focus and are at different stages of maturity, we have developed a separate maturity plan for each program. The maturity plans are provided in Attachment 1.

The maturity plans outline the key initiatives and components used to evaluate the programs. They will allow us to detail the stages of maturity and show our progress towards the goal.

Enterprise Risk Management Plan: The first phase of ERM maturity aims to enhance our internal ERM infrastructure by deploying a software solution that streamlines data collection and maps our risks to our internal controls. This will improve our ability to provide risk analysis and risk reporting to business areas, the ERCC, and to the ARM Committee. We also plan to begin implementing the use of risk appetite statements and key risk indicators in our risk measurement and risk reporting. This will improve how strategic decisions affect our risk profile. We will also be reviewing our charter and reporting structure to see if there are any areas where we can make recommendations for improving how we report risk information to the board and management.

Enterprise Compliance Services Plan: This first phase of the ECS maturity plan focuses on identifying the roles and responsibilities of the compliance teams across the organization, defining the responsibilities of ECS, proposing updates to the reporting structure and charter to reflect those responsibilities, developing a training plan for the ECS team, developing the framework for a monitoring program, and supporting the third-party risk management program. The plan also includes implementing a compliance software solution that leverages the same software as the ERM program. As the ECS team is relatively small, this first 18-month plan is designed to provide the team with awareness of what the organization's compliance responsibilities are, what the organization already does to comply with its various regulatory responsibilities, identify where there may be any gaps, and develop a targeted monitoring program that starts to fill those gaps.

Next steps include working with our Risk Champion Network and business area partners to implement the plan and regular reporting to the ERCC and the ARM Committee on our progress and any challenges.

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
