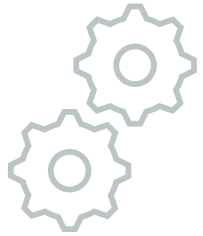
CALSTRS

# Enterprise Compliance Services

## 2022 Risk-Based Enterprise Compliance Services Plan

# Presentation Overview

Integrated Risk Assessment

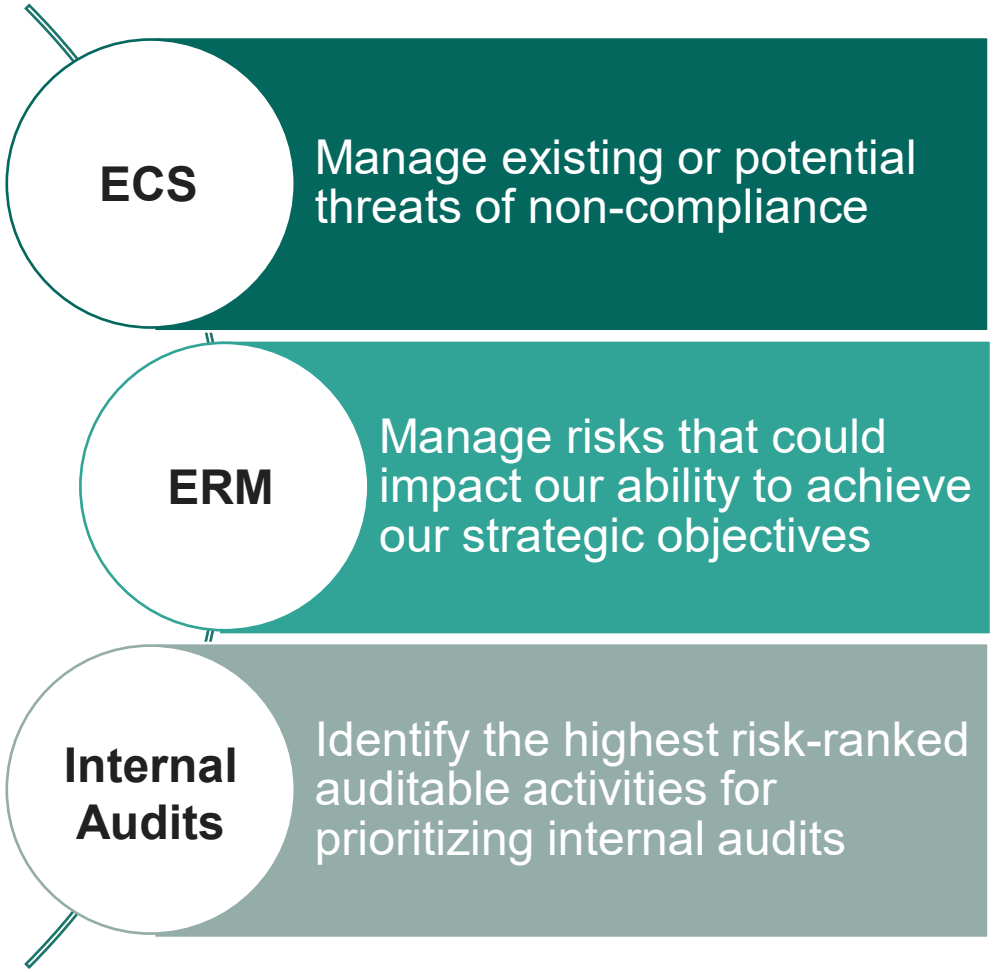


Compliance Risk Assessment

2022 ECS Compliance Plan

# Ongoing Compliance Program Evolution

Aligned with DOJ guidance, ECS has successfully implemented and leveraged an efficient Integrated Risk Assessment Approach to provide the most value and impact at CalSTRS




***Integrated Risk Assessment Approach***

- ✓ Provides foundational & consistent approach
- ✓ Aligns programs on assessment criteria
- ✓ Reduces redundancies
- ✓ Demonstrates maturity
- ✓ Knowledge sharing
- ✓ Better informs risk decision-making

# Compliance Risk Assessment Methodology

Our risk assessment approach intelligently gathers and analyzes risk information to measure our success and inform our compliance risk planning and monitoring activities

**CalSTRS Enterprise Risk Report**

**Branch Operational Annual Risk Assessments**

**Emerging Compliance Risk Insights**

**Review and Update CalSTRS Compliance Risk Taxonomy**

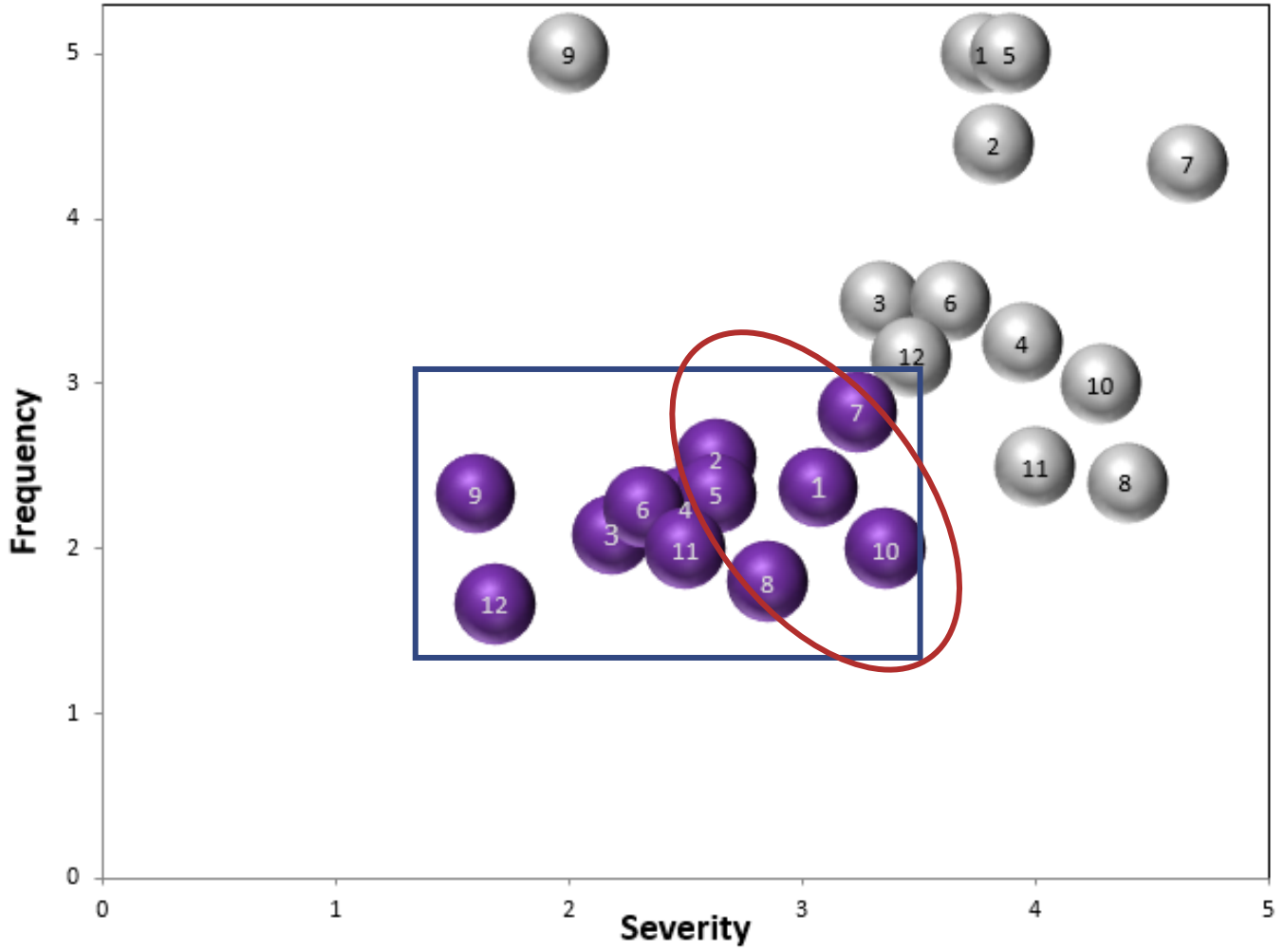
**Conducted 25 Interviews with Leadership for Input on Compliance Risks**

**Utilize Inputs to Quantitatively Score Each Compliance Risk**

**Aggregate Scores to Develop ECS 2022 Compliance Plan**

**Connect High-Priority Items to Monitoring Activities**

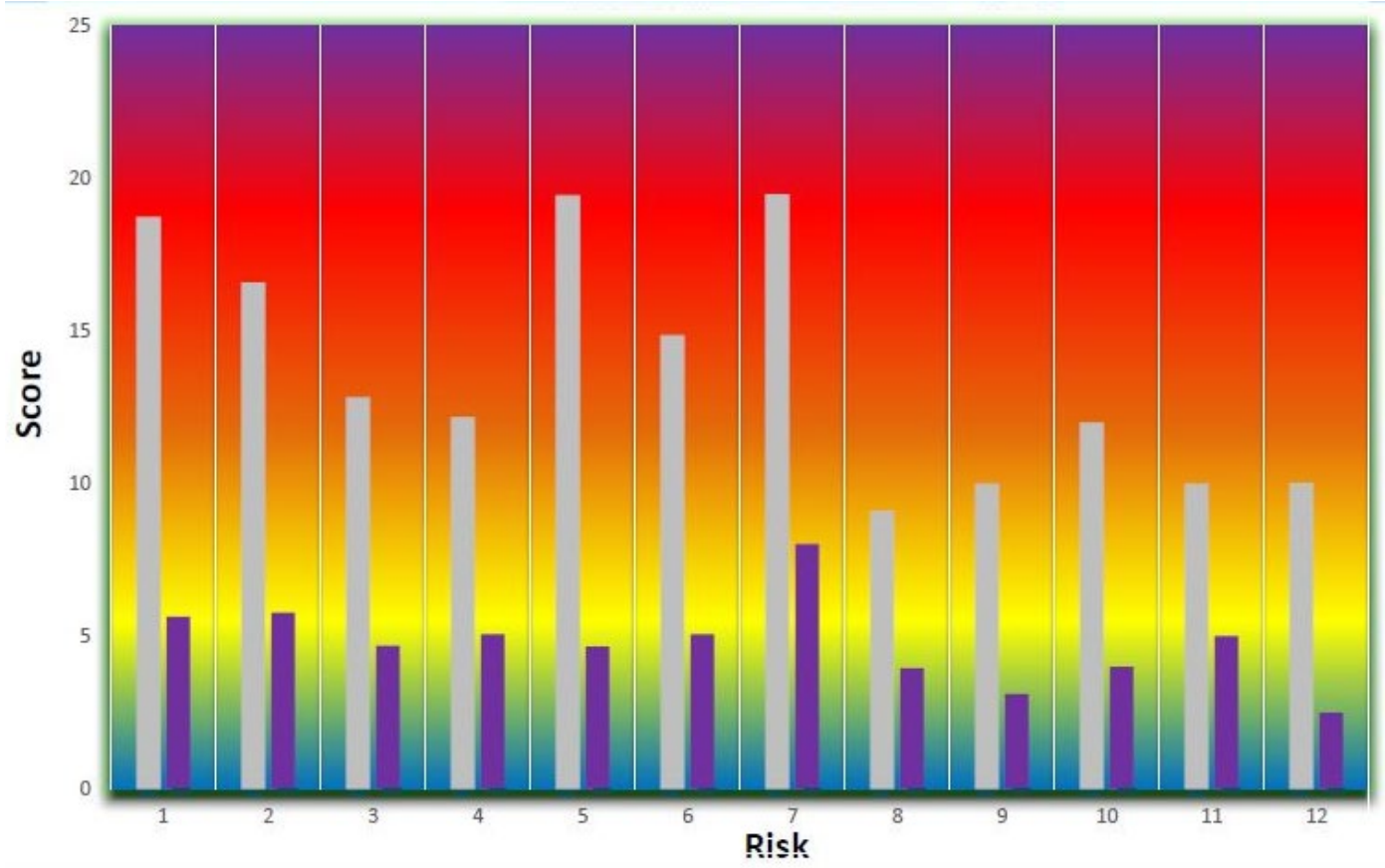
# Compliance Risk Assessment: Material Risk Profile




Ranking by Residual Risk

| # | Material Risk Title |
|---|---|
| 7 | Information Security |
| 1 | Investments |
| 10 | Third Parties |
| 2 | Pension Administration |
| 5 | Financial |
| 8 | Safety, Security, & Resiliency |
| 4 | Information Technology |
| 11 | Ethical Culture |
| 6 | Anti-Bribery & Anti-Corruption |
| 3 | Labor & Employment |
| 9 | Stakeholder Outreach & Social Media |
| 12 | Regulatory / Legal |

# Compliance Risk Assessment: Heatmap Results




| # | Material Risk Title |
|---|---|
| 1 | Investments |
| 2 | Pension Administration |
| 3 | Labor and Employment |
| 4 | Information Technology |
| 5 | Financial |
| 6 | Anti-Bribery and Anti-Corruption |
| 7 | Information Security |
| 8 | Safety, Security & Resiliency |
| 9 | Stakeholder Outreach & Social Media |
| 10 | Third Parties |
| 11 | Ethical Culture |
| 12 | Regulatory/Legal |

**Legend**

= Inherent Risk

= Residual Risk

# Top Compliance Risks and Plan Highlights

Results from the Compliance Risk Assessment align directly to our 2022 ECS Compliance Plan

| Compliance Risk | Specific Sub Risk | Connection to Compliance Plan |
|---|---|---|
| **Information Security** | • Data Privacy<br>• Account Takeovers<br>• Data Governance<br>• Information Security Awareness | ➢ Compliance & Ethics Accountability Matrix<br>➢ Regulatory Tracking Subscription<br>➢ Iterative Compliance Risk Assessment Q3<br>➢ Policy/Standards Reviews & Highlights<br>➢ Participate in Implementation of Governance, Risk & Compliance Tool |
| **Third Parties** | • Third Party Access<br>• Contract Management | ➢ Develop Third-Party/Supplier Code of Conduct<br>➢ Assist Procurement on Contract Management Controls/Tools<br>➢ Collaborate with General Counsel<br>➢ Coordinate/Refine Third-Party System & Organization Controls Reporting Review Process |
| **Investments** | • Asset Allocation<br>• Investment Regulations | ➢ Compliance & Ethics Accountability Matrix<br>➢ Complete Compliance Processes, Legal Requirement and Controls Documentation<br>➢ Regulatory Tracking Subscription<br>➢ Iterative Compliance Risk Assessment Q1<br>➢ Update/Validate External Compliance Reporting |

# Top Compliance Risks and Plan Highlights (Continued)

Results from the Compliance Risk Assessment align directly to our 2022 ECS Compliance Plan

| Compliance Risk | Specific Sub Risk | Connection to Compliance Plan |
|---|---|---|
| **Pension Administration** | • Pension Funding<br>• Defined Contribution<br>• Contribution Rates | ➢ Compliance & Ethics Accountability Matrix<br>➢ Regulatory Tracking Subscription<br>➢ Policy/Standards Reviews<br>➢ Communication Guides for Leaders on Compliance Obligations<br>➢ Iterative Compliance Risk Assessment Q1 |
| **Safety, Security & Resiliency** | • Environmental Hazards<br>• Employee Health & Safety | ➢ Develop Compliance Processes, Legal Requirement and Controls Documentation<br>➢ Compliance & Ethics Accountability Matrix<br>➢ Regulatory Tracking Subscription<br>➢ Policy/Standards Reviews<br>➢ Iterative Compliance Risk Assessment Q1<br>➢ Update/Validate External Compliance Reporting |
| **Financial** | • Tax Requirements<br>• Budget/Cash Management | ➢ Compliance & Ethics Accountability Matrix<br>➢ Regulatory Tracking Subscription<br>➢ Policy/Standards Reviews<br>➢ Iterative Compliance Risk Assessment Q2<br>➢ Update/Validate External Financial Compliance Reporting |

# Final Thoughts

# Appendix

- Top Compliance Risk and Sub Risks
- Enterprise Compliance Risk Definitions
- Structure of Compliance Risks

# Top Compliance Risks and Related Sub Risks

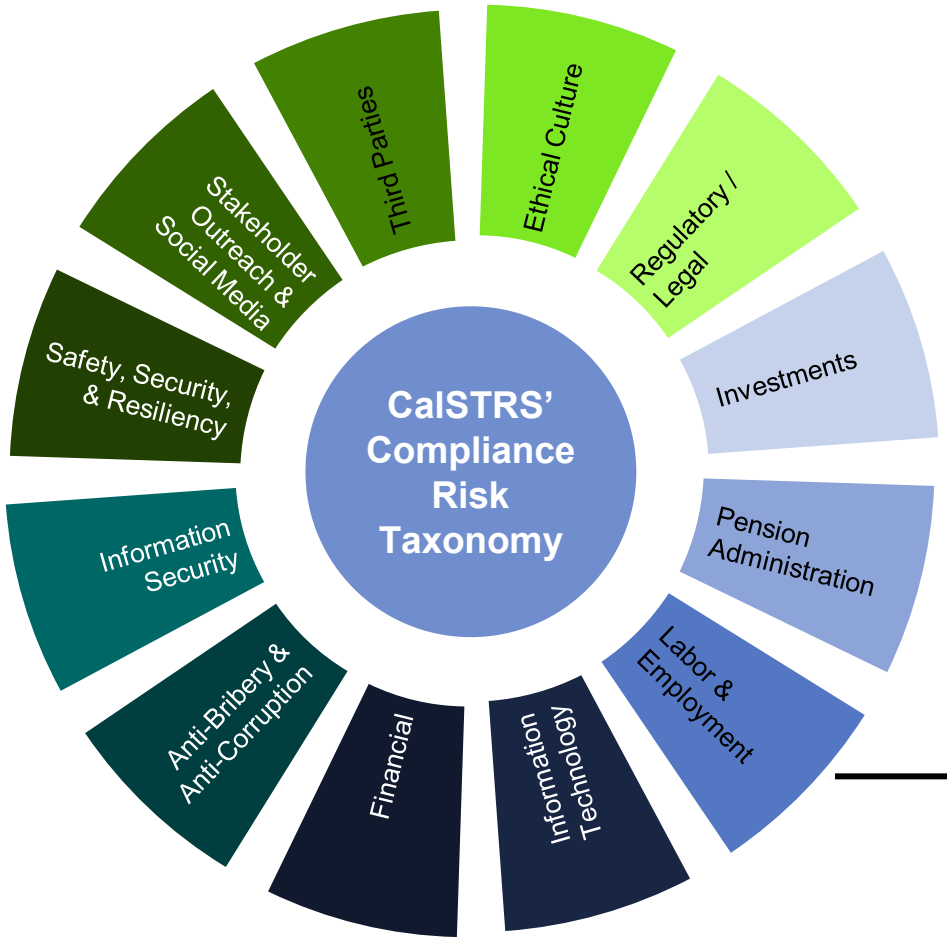
| Information Security | Third Parties | Pension Administration | Financial | Investments | Safety, Security & Resiliency |
|---|---|---|---|---|---|
| • Data Privacy<br>• Data Breach Response<br>• Records Management<br>• Data Governance<br>• Account Takeovers<br>• Information Security Awareness | • Fair Procurement Practices<br>• Procurement Conflict of Interest<br>• Vendor Due Diligence & Selection<br>• Third Party Access<br>• Contract Management<br>• Contract Expiration | • Actuarial Standards<br>• Actuarial Assumptions<br>• Pension Funding<br>• Contribution Rates<br>• Reporting / Collection of Contributions<br>• Accurate Benefit Payments<br>• Benefit Payment-Appeals<br>• Employer Reporting<br>• Defined Contribution<br>• Penalties & Interest<br>• Customer Service | • Tax Requirements<br>• Master Custodian Reconciliation<br>• Auditing & Accounting Standards<br>• Legislative Required Financial Reporting<br>• Assurance<br>• Accounting-Payments<br>• Accounting-Receivables<br>• Budget / Cash Management<br>• Fraud | • Asset Allocation<br>• Fiscal Transparency<br>• Investment Regulations<br>• Asset Class Threshold<br>• Restricted Investments<br>• Insider Trading & Market Manipulation | • Environmental Hazards<br>• Physical Security<br>• Building Access<br>• Employee Health & Safety<br>• Business Continuity |

# Enterprise Compliance Material Risk Definitions

| Ref # | Compliance Risk Name | Risk Definition |
|---|---|---|
| 1.0 | Investments | The potential for CalSTRS or third party acting on its behalf to not comply with applicable investment compliance regulations and agency guidance. |
| 2.0 | Pension Administration | The potential for CalSTRS or third party acting on its behalf to irresponsibly/negligently administer pension in a way that would prevent CalSTRS from keeping the organization's pension fund solvent. |
| 3.0 | Labor and Employment | The potential for CalSTRS or third party acting on its behalf to not be in compliance with applicable CalSTRS policies and state and federal laws or regulations. |
| 4.0 | Information Technology | The potential for CalSTRS or third party acting on its behalf to improperly protect, access or use internal CalSTRS data or information technology systems. |
| 5.0 | Financial | The potential for CalSTRS or third party acting on its behalf to knowingly contribute to incorrect or fraudulent financial disclosures, not to comply with accounting regulations; falsification of information in any way, whether for distribution internally or externally, or noncompliance with SEC requirements and statutory requirements. |
| 6.0 | Anti-Bribery and Anti-Corruption | The potential for CalSTRS or third party acting on its behalf to offer, promise, provide, or receive anything of value to or from any third party (including a government official or commercial business partner) for the purposes of gaining or maintaining an unfair competitive advantage. |
| 7.0 | Information Security | The potential for CalSTRS or third party acting on its behalf to improperly protect or misuse CalSTRS or its members' data. |
| 8.0 | Safety, Security & Resiliency | The potential for CalSTRS or third party acting on its behalf to compromise the protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to CalSTRS employees, individual members, third parties, or the enterprise. |
| 9.0 | Stakeholder Outreach & Social Media | The potential for CalSTRS or third party acting on its behalf to utilize a social media platform (e.g., Facebook) to communicate confidential information on behalf of CalSTRS or to inappropriate represent CalSTRS on a social media platform without authorization, permission, or approval. |
| 10.0 | Third Parties | The potential for CalSTRS to hire, retain, engage, or partner with a third party, without having designed and implemented appropriate controls intended to manage risk throughout the lifecycle of third-party relationships. |
| 11.0 | Ethical Culture | The potential for the CalSTRS workforce to not be aware of or understand CalSTRS ethical and compliance expectations and obligations resulting in noncompliance, loss of public trust, and degradation of culture. |
| 12.0 | Regulatory/Legal | The potential for CalSTRS or third party acting on its behalf to fail to track, monitor, and comply with evolving laws and regulations on a consistent and regular basis, or provide timely updates to policies, procedures and trainings to reflect new legal and regulatory requirements. |

# CalSTRS Compliance Risk Taxonomy

Our existing risk taxonomy captures all the risks that could have a major impact at CalSTRS. In the taxonomy, risks are tiered into three levels, allowing for improved risk management by risk owners.




Interview participants were asked to discuss and score individual subcomponent and principal risks.