weaver
Assurance • Tax • Advisory

# Enterprise Risk Management and Compliance Services Maturity Assessment Executive Summary

California State Teachers' Retirement System | February 2023

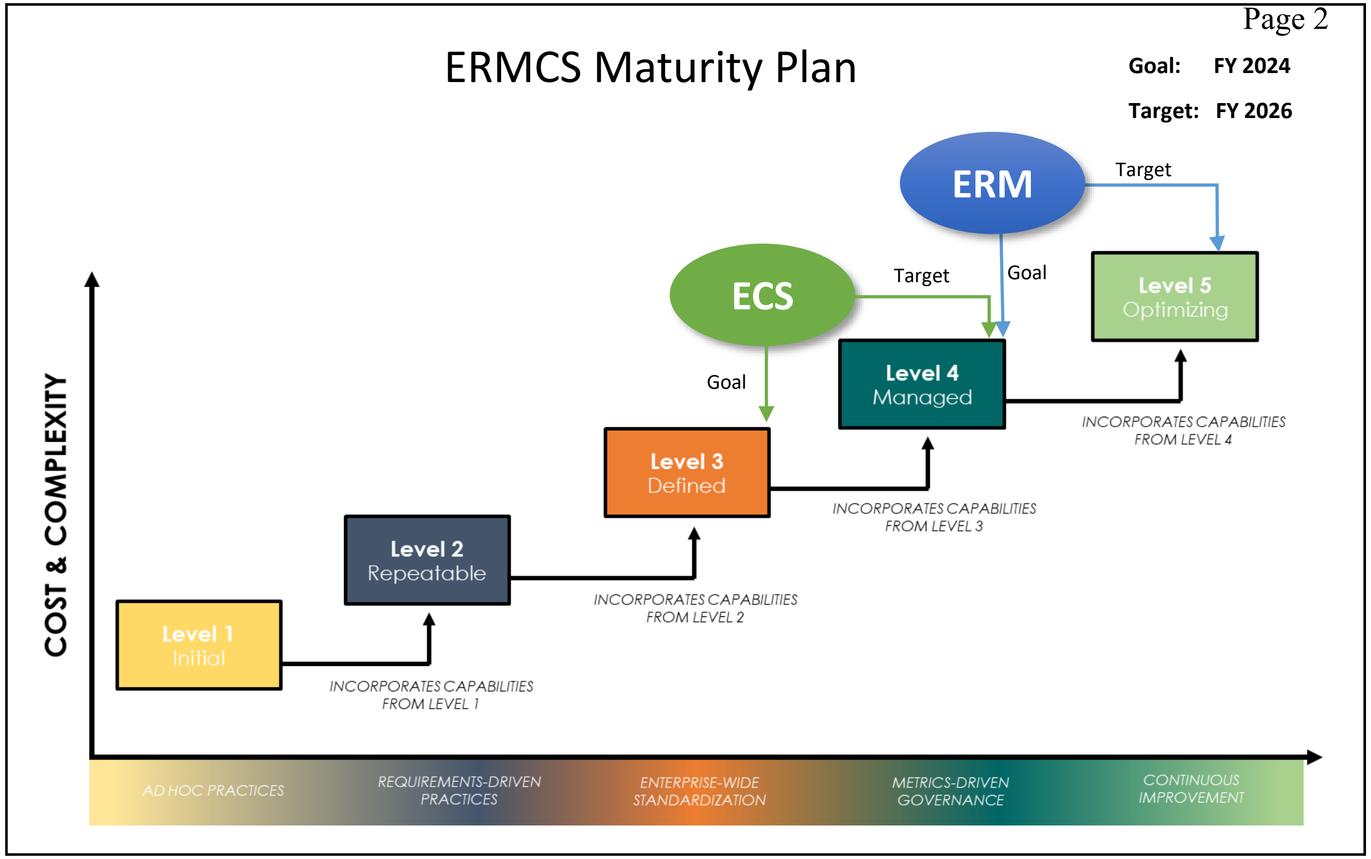
# Approach

Weaver evaluated the maturity of the Enterprise Risk Management (ERM) and Enterprise Compliance Services (ECS) functions for CalSTRS 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.

The primary purpose of the review was to show the current levels of maturity for each function to inform the roadmap to the future state on both a short and long term basis.

Our approach included:

1. Evaluation of the ERM and ECS programs against **COSO** and **SCCE** Frameworks
   - 6 key components, 20+ principles, and 95+ evaluation criteria for each framework
   - **Standard requirements for an effective ERM and Compliance Program**
2. Set Goal and Target **Maturity expectation** with Management for both ERM and ECS
3. Interviews with key executives and Trustees
4. Assessment of the **knowledge, skills and abilities** of the personnel
5. Surveys with the internal Risk Champions Network and CalSTRS' peers to
   - Inform the risk **culture, effectiveness, and overall integration** of ERM
   - Provide a comparison of how peers have approached both areas
6. Development of a **future state roadmap** of actions, benefits, challenges, and key implementation steps for ERM and ECS to achieve their desired maturity levels on a short and long-term basis.



ERMCS Maturity Plan

**Goal:** **FY 2024**

**Target:** **FY 2026**

ERM
Target
Goal
ECS
Target
Goal
COST & COMPLEXITY
Level 1
Initial
Level 2
Repeatable
Level 3
Defined
Level 4
Managed
Level 5
Optimizing
INCORPORATES CAPABILITIES FROM LEVEL 1
INCORPORATES CAPABILITIES FROM LEVEL 2
INCORPORATES CAPABILITIES FROM LEVEL 3
INCORPORATES CAPABILITIES FROM LEVEL 4
AD HOC PRACTICES
REQUIREMENTS-DRIVEN PRACTICES
ENTERPRISE-WIDE STANDARDIZATION
METRICS-DRIVEN GOVERNANCE
CONTINUOUS IMPROVEMENT

Organizations ***should expect*** that moving from each level of maturity includes additional components of:

- Cost
- Complexity
- Advanced Business Practices

# Summary of Results

To successfully achieve the increased maturity levels for ERM and ECS, there were four themes identified. Addressing these themes will accelerate the maturity process.

1. **Risk Appetite and Risk Tolerance**
   Defining risk appetite and risk tolerance, which are fundamental building blocks of ERM, brings the organization closer to fully integrating ERM into the formulation of business objectives and alignment with the strategic goals of the organization.

2. **Compliance Access and Authority**
   ECS will need the authority and access to effectively oversee compliance activities including those in the distributed compliance functions within branches. As the team matures, they could begin to assume ownership of compliance-related policies, monitoring, compliance training, and additional involvement during investigations and actions related to compliance issues.

3. **Advanced ERM Integration**
   ERM's structure broadly covers the expected principles of the COSO framework. To reach a higher maturity level, ERM will require an increased level of integration and technology across most of their current processes to become a predictable, measured, metrics-driven function. This involves additional KRIs, data-driven metrics, structured risk response, and establishing risk priorities. The Risk Champions will continue to need support from their executives and teams to help drive this development.

4. **Resources**
   As the functions evolve, so must their resources. This includes people, process, and technology. Employees would benefit from additional training, opportunities to demonstrate proficiency through certifications, and being properly situated to fully understand the branches various lines of business. Access to data and systems will be needed to leverage existing technology. Both areas are properly staffed for their current roles, but CalSTRS will have to assess the staffing needs to grow the maturity and capabilities.

These themes and the assessment also identified specific **actionable opportunities** to accelerate both ERM's and ECS' pace towards achieving their maturity goals and targets

**Enterprise Risk Management**

1. Define and Implement Risk Appetite and Risk Tolerance
2. Prioritize Risks and Implement 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

**Enterprise Compliance Services**

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

These actionable opportunities provide CalSTRS a potential roadmap that includes specific actions, benefits, challenges and key implementation steps recommended to move both ERM and ECS towards increased program maturity. Detailed evaluations of progress towards the desired maturity levels for each principle in the framework were provided to ERM/ECS in a separate report.

# Current State Maturity Assessment

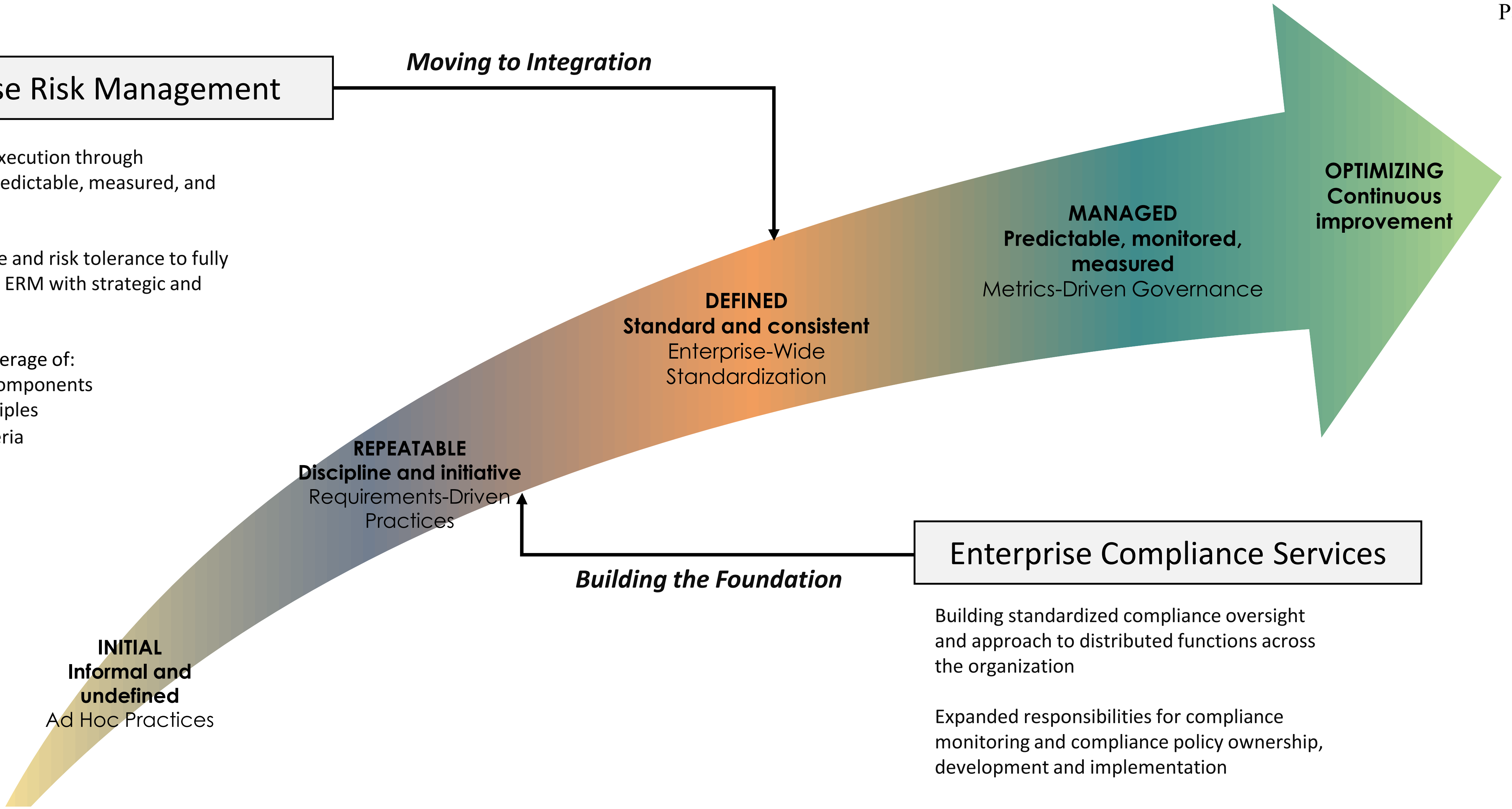
## Enterprise Risk Management

Mature program execution through technology with predictable, measured, and monitored metrics

Define risk appetite and risk tolerance to fully integrate and align ERM with strategic and business planning

ERM has some coverage of:

- 6 of 6 ERM Components
- 21 of 21 Principles
- 94 of 98 Criteria



*Moving to Integration*

**INITIAL**
**Informal and undefined**
Ad Hoc Practices

**REPEATABLE**
**Discipline and initiative**
Requirements-Driven Practices

**DEFINED**
**Standard and consistent**
Enterprise-Wide Standardization

**MANAGED**
**Predictable, monitored, measured**
Metrics-Driven Governance

**OPTIMIZING**
**Continuous improvement**

*Building the Foundation*

## Enterprise Compliance Services

Building standardized compliance oversight and approach to distributed functions across the organization

Expanded responsibilities for compliance monitoring and compliance policy ownership, development and implementation

ECS has some coverage of:

- 6 of 6 ECS Components
- 22 of 22 Principles
- 89 of 95 Criteria

# Maturity Models – Components and Principles

The graphic at right shows the key components and principles used within the maturity assessment of ERM and ECS.

These were developed 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.

**Enterprise Risk Management**

| COMPONENTS | | | | | |
|---|---|---|---|---|---|
| **Governance and Culture** | **Strategy and Objectives** | **Performance** | **Review and Revision** | **Communication and Reporting** | **Technology** |
| PRINCIPLES | | | | | |
| Authority and Organizational Commitment | Analyzes Business Context | Risk Identification | Assesses Substantial Change | Communicates Risk Information | Leverages Information Systems |
| Board Oversight for Risk | Risk Appetite | Assesses Severity of Risk | Reviews Risk and Performance | Reports on Risk, Culture, and Performance | |
| Established Operating Structure | Strategic Alignment | Risk Tolerance and Prioritization | Pursues Improvement in ERM | | |
| Desired Culture Defined | Formulates Business Objectives | Implements Risk Responses | | | |
| Demonstrated Commitment to Core Values | | Develops Portfolio View | | | |
| Attracts, Develops, and Retains Top Talent | | | | | |

| COMPONENTS | PRINCIPLES | CRITERIA |
|---|---|---|
| 6 | 21 | 98 |

**Enterprise Compliance Services**

| COMPONENTS | | | | | |
|---|---|---|---|---|---|
| **Governance, Administration and Reporting** | **Standards and Policies** | **Risk Assessment and Monitoring** | **Enforcement and Response** | **Training and Education** | **Technology** |
| PRINCIPLES | | | | | |
| Compliance Authority | Administrative Oversight of Policies | Risk Assessment | Reporting Channels | Compliance Education Program | Support |
| Compliance Committee | Regulatory Understanding | Compliance Monitoring | Investigation Processes | Training Plan Administration | Capabilities |
| Authority and Administration | Administration and Communication | Combined Assurance Model | Disciplinary Guidelines | Continuing Education | |
| Reporting and Education | Compliance-owned Policies | | Employee Communication | | |
| Enforcement and Response | | | | | |
| Resources | | | | | |

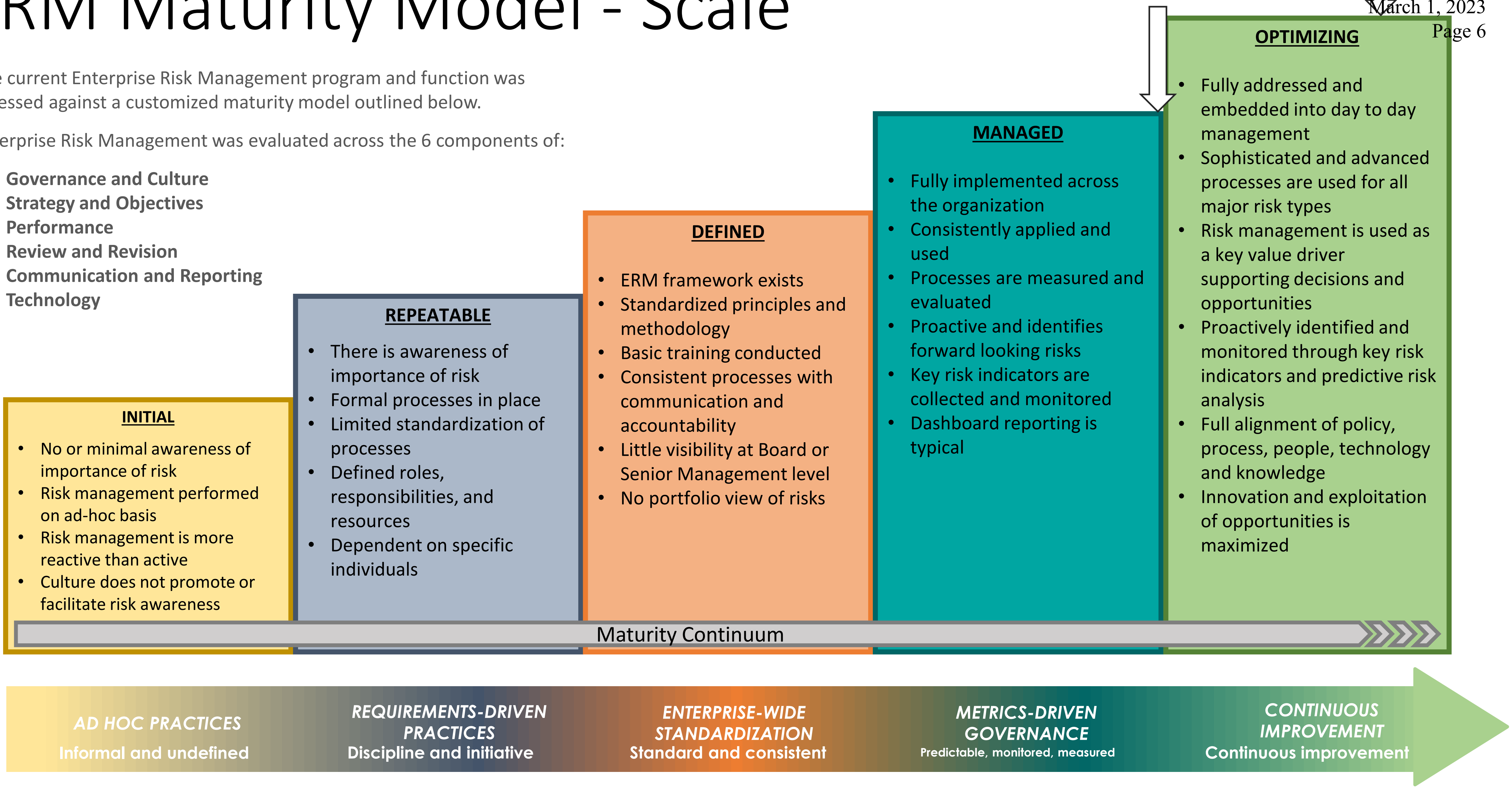
| COMPONENTS | PRINCIPLES | CRITERIA |
|---|---|---|
| 6 | 22 | 95 |

# ERM Maturity Model - Scale

The current Enterprise Risk Management program and function was assessed against a customized maturity model outlined below.

Enterprise Risk Management was evaluated across the 6 components of:

1. **Governance and Culture**
2. **Strategy and Objectives**
3. **Performance**
4. **Review and Revision**
5. **Communication and Reporting**
6. **Technology**



**INITIAL**

- No or minimal awareness of importance of risk
- Risk management performed on ad-hoc basis
- Risk management is more reactive than active
- Culture does not promote or facilitate risk awareness

**REPEATABLE**

- There is awareness of importance of risk
- Formal processes in place
- Limited standardization of processes
- Defined roles, responsibilities, and resources
- Dependent on specific individuals

**DEFINED**

- ERM framework exists
- Standardized principles and methodology
- Basic training conducted
- Consistent processes with communication and accountability
- Little visibility at Board or Senior Management level
- No portfolio view of risks

**MANAGED**

- Fully implemented across the organization
- Consistently applied and used
- Processes are measured and evaluated
- Proactive and identifies forward looking risks
- Key risk indicators are collected and monitored
- Dashboard reporting is typical

**OPTIMIZING**

- Fully addressed and embedded into day to day management
- Sophisticated and advanced processes are used for all major risk types
- Risk management is used as a key value driver supporting decisions and opportunities
- Proactively identified and monitored through key risk indicators and predictive risk analysis
- Full alignment of policy, process, people, technology and knowledge
- Innovation and exploitation of opportunities is maximized

*AD HOC PRACTICES*
Informal and undefined

*REQUIREMENTS-DRIVEN PRACTICES*
Discipline and initiative

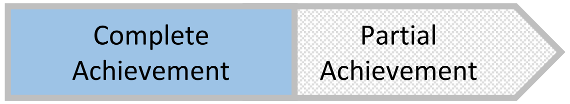
*ENTERPRISE-WIDE STANDARDIZATION*
Standard and consistent

*METRICS-DRIVEN GOVERNANCE*
Predictable, monitored, measured

*CONTINUOUS IMPROVEMENT*
Continuous improvement

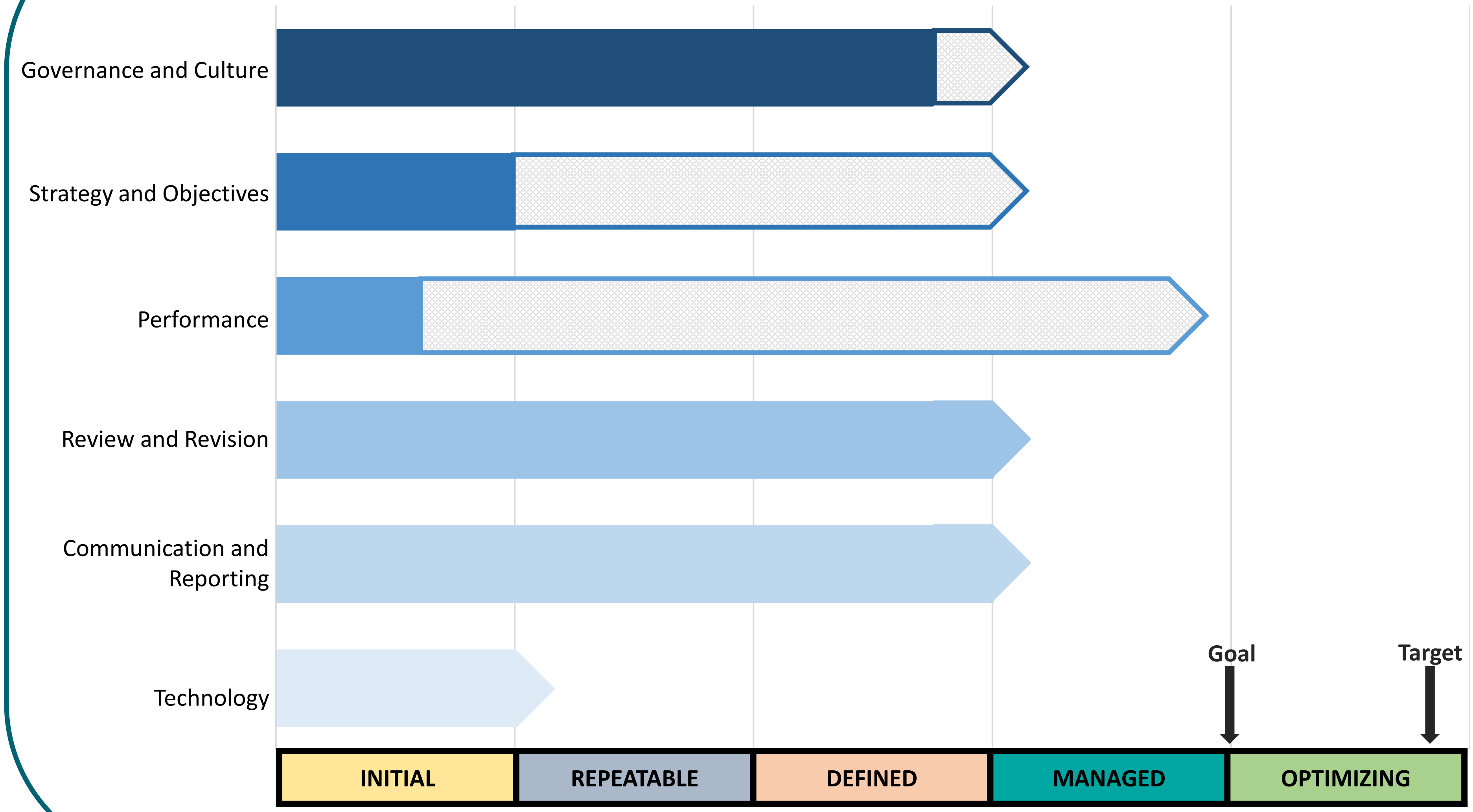
The graphic at right highlights the current overall status of CalSTRS **Enterprise Risk Management** program, together with the Goal and Target Maturity levels for the program based on a 3-year time horizon.

Furthermore, the image depicts the level of progress toward achieving the **next highest maturity level** for each component.

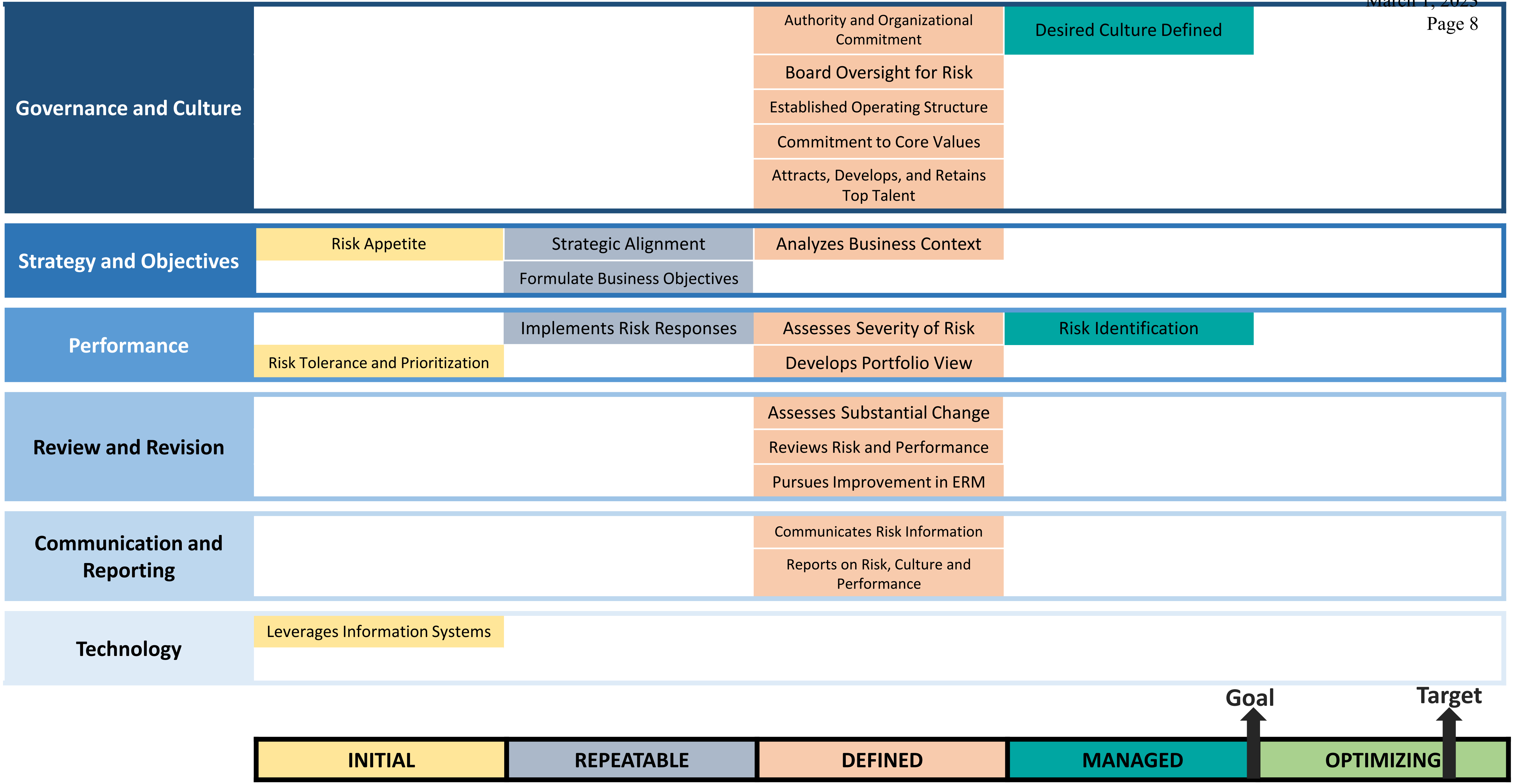


Enterprise Risk Management

**Overall Maturity Achievement**



# ERM Maturity Model – Current State



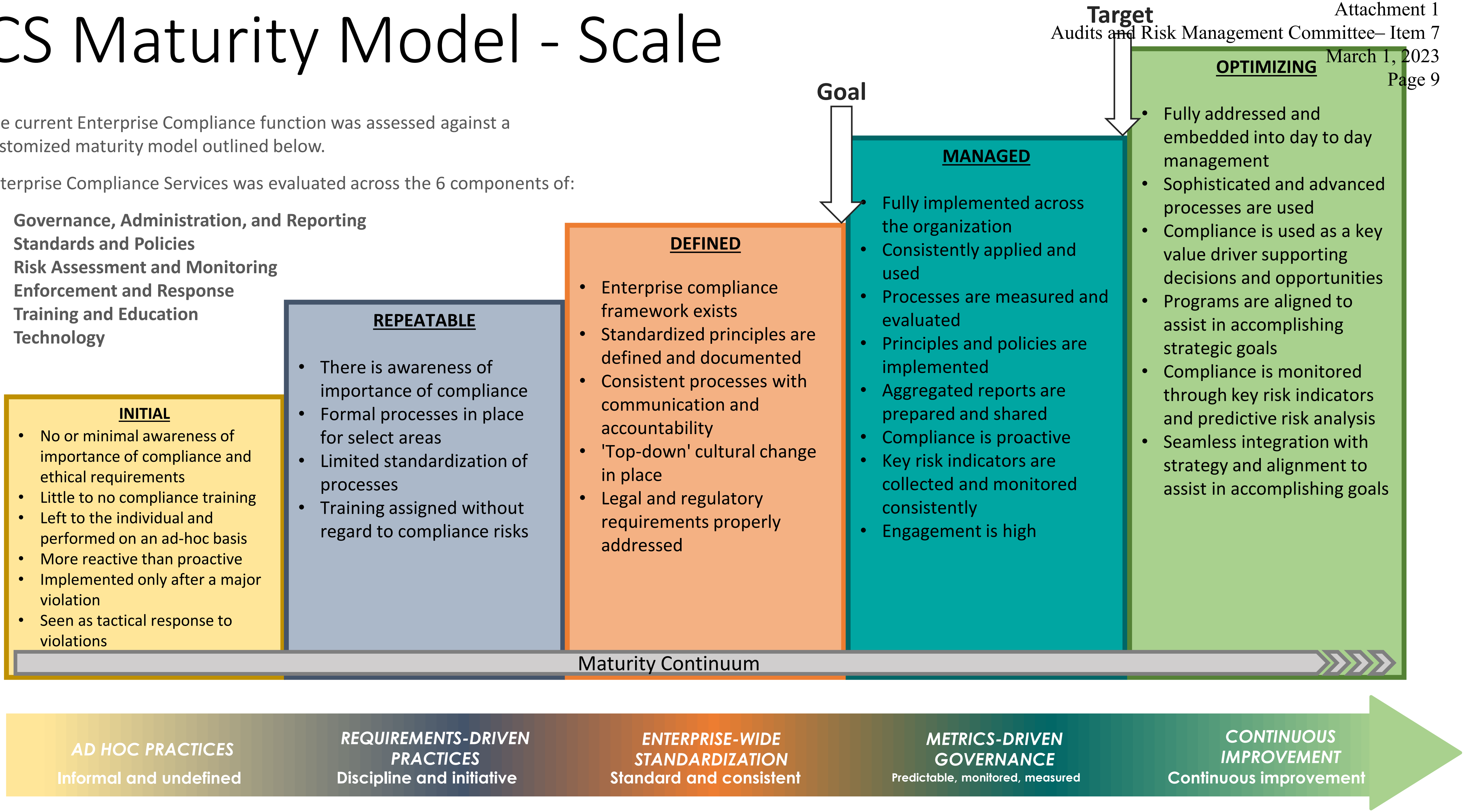
| | INITIAL | REPEATABLE | DEFINED | MANAGED | OPTIMIZING |
|---|---|---|---|---|---|
| Governance and Culture | | | Authority and Organizational Commitment<br>Board Oversight for Risk<br>Established Operating Structure<br>Commitment to Core Values<br>Attracts, Develops, and Retains Top Talent | Desired Culture Defined | |
| Strategy and Objectives | Risk Appetite | Strategic Alignment<br>Formulate Business Objectives | Analyzes Business Context | | |
| Performance | Risk Tolerance and Prioritization | Implements Risk Responses | Assesses Severity of Risk<br>Develops Portfolio View | Risk Identification | |
| Review and Revision | | | Assesses Substantial Change<br>Reviews Risk and Performance<br>Pursues Improvement in ERM | | |
| Communication and Reporting | | | Communicates Risk Information<br>Reports on Risk, Culture and Performance | | |
| Technology | Leverages Information Systems | | | | |

# ECS Maturity Model - Scale

The current Enterprise Compliance function was assessed against a customized maturity model outlined below.

Enterprise Compliance Services was evaluated across the 6 components of:

1. **Governance, Administration, and Reporting**
2. **Standards and Policies**
3. **Risk Assessment and Monitoring**
4. **Enforcement and Response**
5. **Training and Education**
6. **Technology**



**Goal**

**Target**

**INITIAL**

- No or minimal awareness of importance of compliance and ethical requirements
- Little to no compliance training
- Left to the individual and performed on an ad-hoc basis
- More reactive than proactive
- Implemented only after a major violation
- Seen as tactical response to violations

**REPEATABLE**

- There is awareness of importance of compliance
- Formal processes in place for select areas
- Limited standardization of processes
- Training assigned without regard to compliance risks

**DEFINED**

- Enterprise compliance framework exists
- Standardized principles are defined and documented
- Consistent processes with communication and accountability
- 'Top-down' cultural change in place
- Legal and regulatory requirements properly addressed

**MANAGED**

- Fully implemented across the organization
- Consistently applied and used
- Processes are measured and evaluated
- Principles and policies are implemented
- Aggregated reports are prepared and shared
- Compliance is proactive
- Key risk indicators are collected and monitored consistently
- Engagement is high

**OPTIMIZING**

- Fully addressed and embedded into day to day management
- Sophisticated and advanced processes are used
- Compliance is used as a key value driver supporting decisions and opportunities
- Programs are aligned to assist in accomplishing strategic goals
- Compliance is monitored through key risk indicators and predictive risk analysis
- Seamless integration with strategy and alignment to assist in accomplishing goals

Maturity Continuum

*AD HOC PRACTICES*
Informal and undefined

*REQUIREMENTS-DRIVEN PRACTICES*
Discipline and initiative

*ENTERPRISE-WIDE STANDARDIZATION*
Standard and consistent

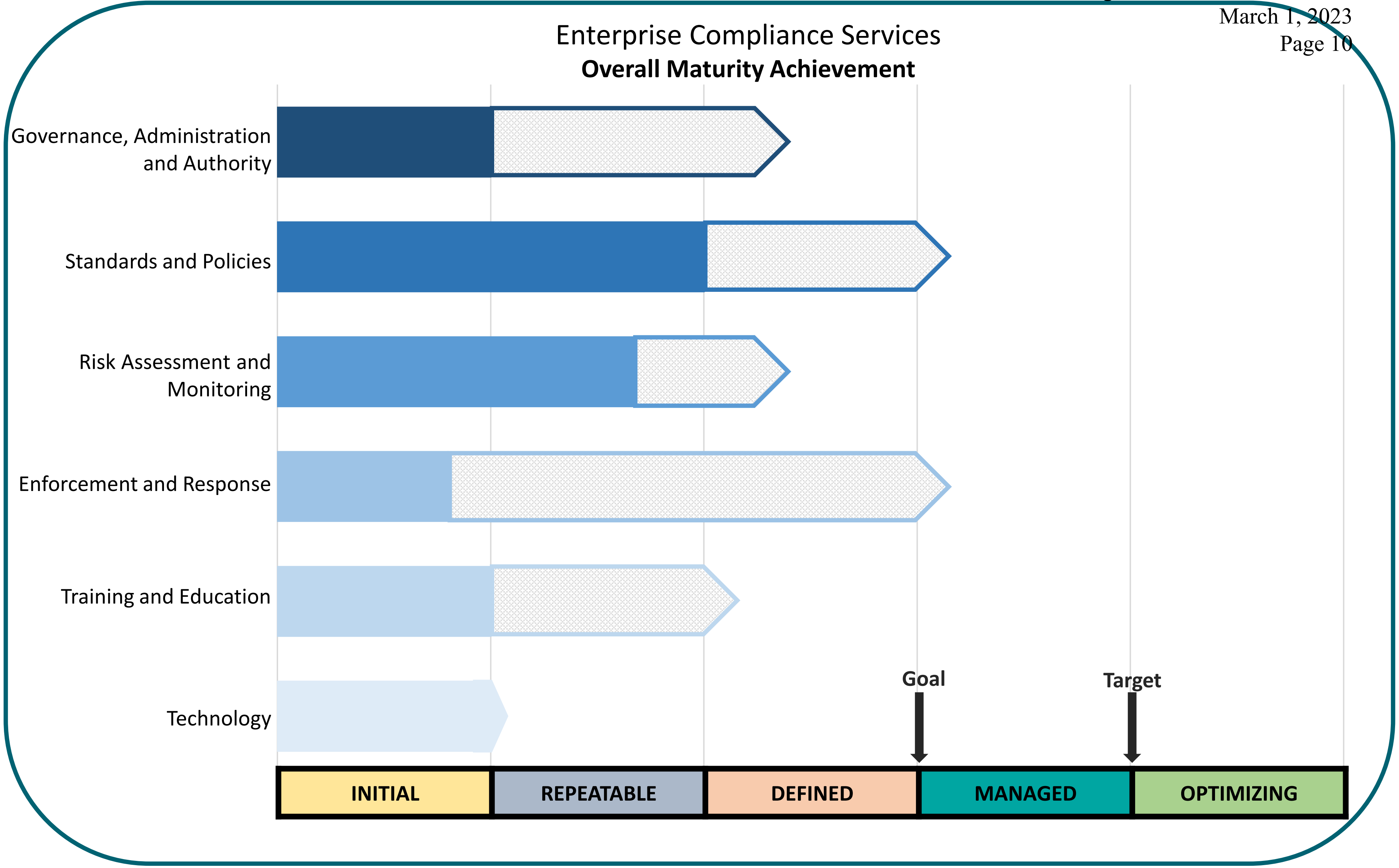
*METRICS-DRIVEN GOVERNANCE*
Predictable, monitored, measured

*CONTINUOUS IMPROVEMENT*
Continuous improvement

The graphic at right highlights the current overall status of CalSTRS **Enterprise Compliance Services** program, together with the Goal and Target Maturity levels for the program based on the 3-year time horizon.

Furthermore, the image depicts the level of progress toward achieving the **next highest maturity level** for each component.

Complete Achievement | Partial Achievement



# ECS Maturity Model – Current State

| | INITIAL | REPEATABLE | DEFINED | MANAGED | OPTIMIZING |
|---|---|---|---|---|---|
| Governance, Administration and Reporting | | Authority and Administration | Compliance Authority | | |
| | Enforcement and Response | Reporting and Education | | | |
| | | Resources | | | |
| Standards and Policies | | Regulatory Understanding | Administrative Oversight of Policies | | |
| | | Compliance-owned Policies | Administration and Communication | | |
| Risk Assessment and Monitoring | | Compliance Monitoring | Risk Assessment | | |
| | | Combined Assurance Model | | | |
| Enforcement and Response | Investigation Processes | | Reporting Channels | | |
| | Disciplinary Guidelines | | Employee Communication | | |
| Training and Education | Continuing Education | Compliance Education Program | | | |
| | | Training Plan Administration | | | |
| Technology | Support | | | | |
| | Capabilities | | | | |

Goal

Target

INITIAL | REPEATABLE | DEFINED | MANAGED | OPTIMIZING