Enterprise Risk Management & Compliance Services Framework and Maturity Recommendations

March 2023

CalSTRS strategic plan linkage

Goal 1: Objective E

Enhance how risks are defined, viewed and managed.

Assess the mandate and scope of the Enterprise Risk Management and Enterprise Compliance Services programs and identify opportunities to **mature the programs**.

Goal 3: Objective D

Sustainable organization

Strengthen preparedness capabilities to address change and disruptions

CalSTRS Enterprise Risk Management Framework

Component 1: GOVERNANCE

Teachers' Retirement Board

The trustees have ultimate responsibility and accountability for risks.

Executive Risk and Compliance Committee

ERM Program oversight and clearinghouse for risk policy, appetite-setting and governance.

Component 2: PEOPLE, PROCESS, DATA AND TECHNOLOGY

Business Area Risk Owners (Risk Champions, Managers & Staff)	**Aligned Assurance Groups** (ERM, ECS, Information Security)	**Internal and External Audits**
Identifies and take actions to reduce risks.	Provides expertise, support, analysis and reports on the management of risks to the board, ERC and CalSTRS senior management.	Provides independent assurance to the board and CalSTRS senior management on risk management.

*Risk mitigation and compliance requires the collective effort and support **of all CalSTRS employees**.*

ERM current responsibilities

ERM Current Workload and Responsibilities

- Identify emerging and existential risks
- branch risk assessment
- Risk matrix reporting
- Risk champions network
- Enterprise risk training
- State Leadership and Accountability Act (SLAA) reporting

ECS current responsibilities

ECS Current Workload and Responsibilities

- Enterprise policy management*
- Ethics hotline administration
- Service Organization Controls (SOC) monitoring
- Compliance risk assessment
- Enterprise compliance training

**Excluding investment and board policies.*

Summary of Weaver's maturity assessment process

1) Assess current state of ERM and ECS programs

- Reviewed existing ERM/ECS charters, policies, reporting, and structure
- Reviewed previous audit of ERM
- Interviewed internal business partners (Investments, Legal, Operations, IT, Audit, Strategy, etc.)
- Performed knowledge and skills assessment of ERM/ECS staff
- Conducted a Risk Champion survey

2) Measure current state against best practices and peers

- Compared best practice maturity models to ERM and ECS programs
- Conducted peer benchmarking survey

3) Identify areas for improvement

4) Develop recommendations

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					

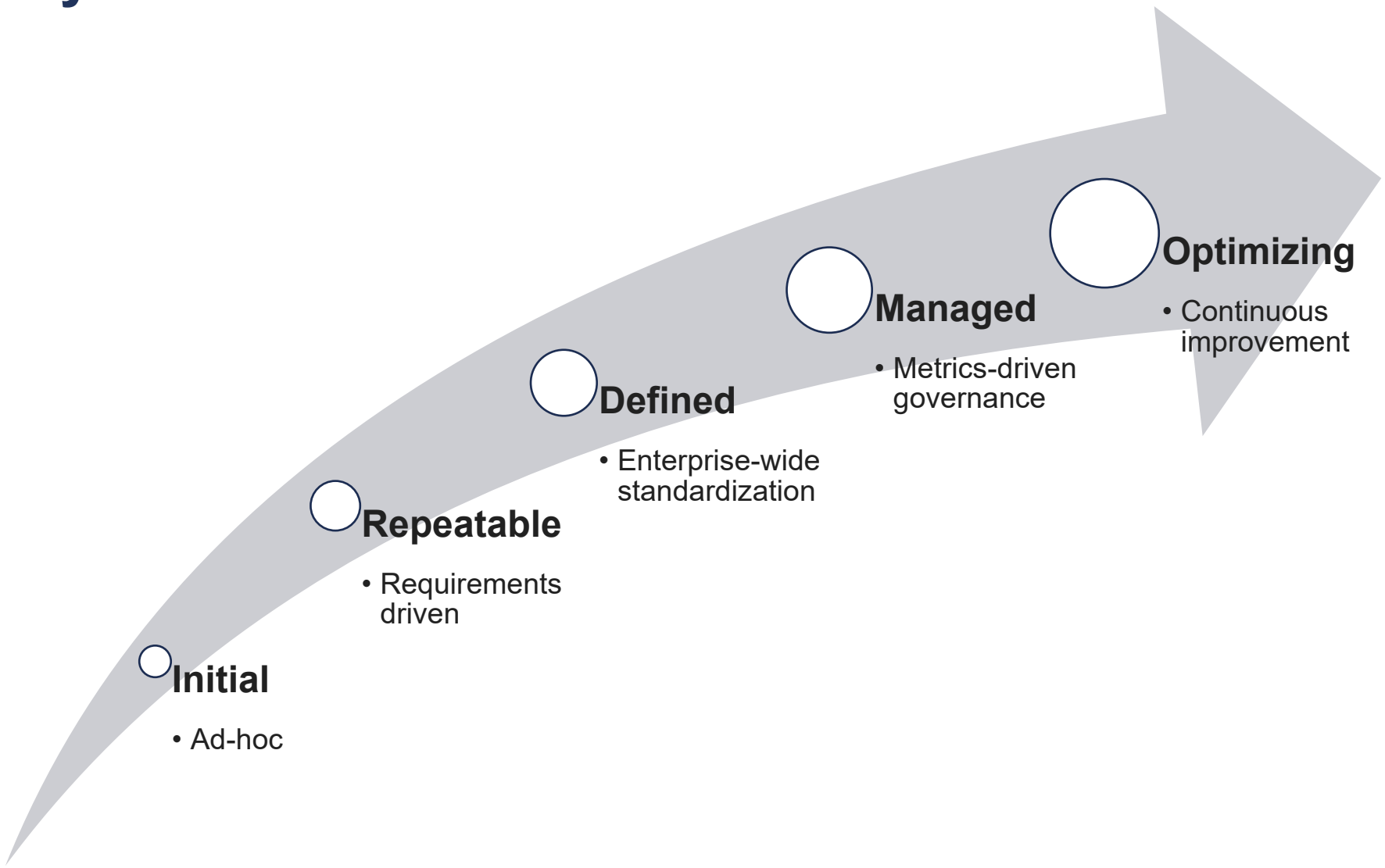
COMPONENTS	PRINCIPLES	CRITERIA
6	21	98

Enterprise Compliance Services

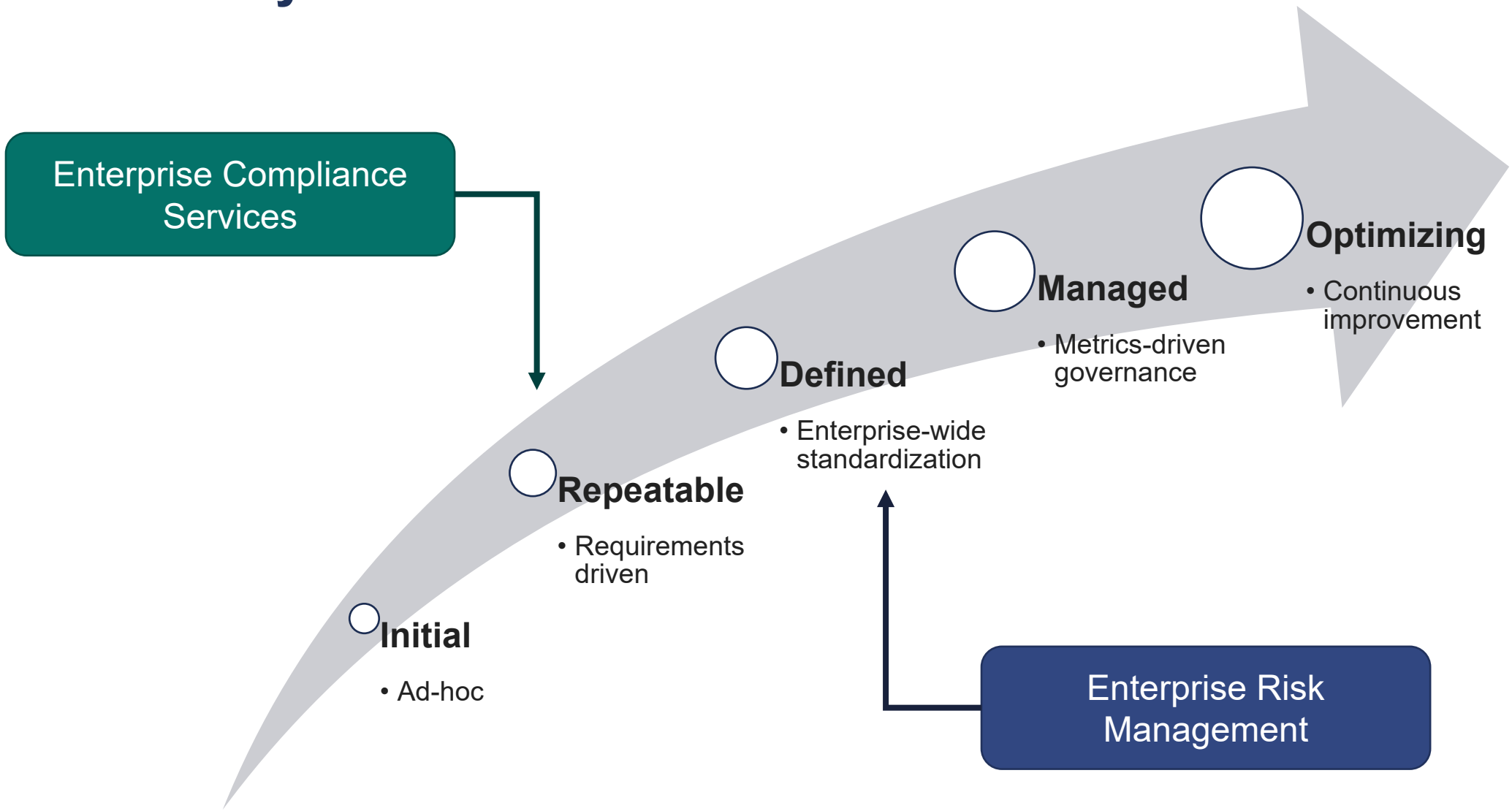
COMPONENTS					
Governance, Administration and Reporting	Standards and Policies	Risk Assessment and Monitoring	Enforcement and Response	Training and Education	Technology
PRINCIPLES					
Compliance Authority	Administrative Oversight of Policies	Risk Assessment	Reporting Channels	Compliance Education Program	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

Maturity Model: Overview



Maturity model: Current state



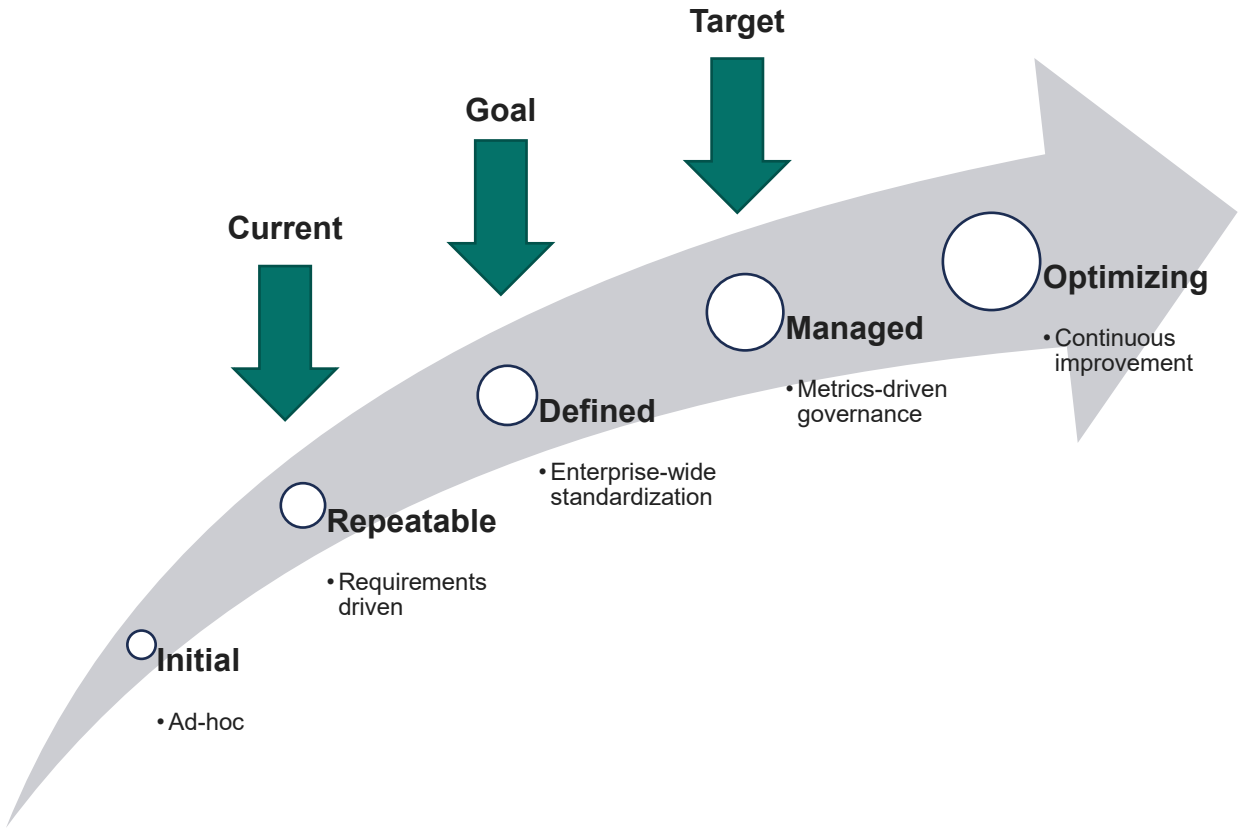
Summary of key areas for improvement

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

Recommendations: ECS

Enterprise Compliance Services

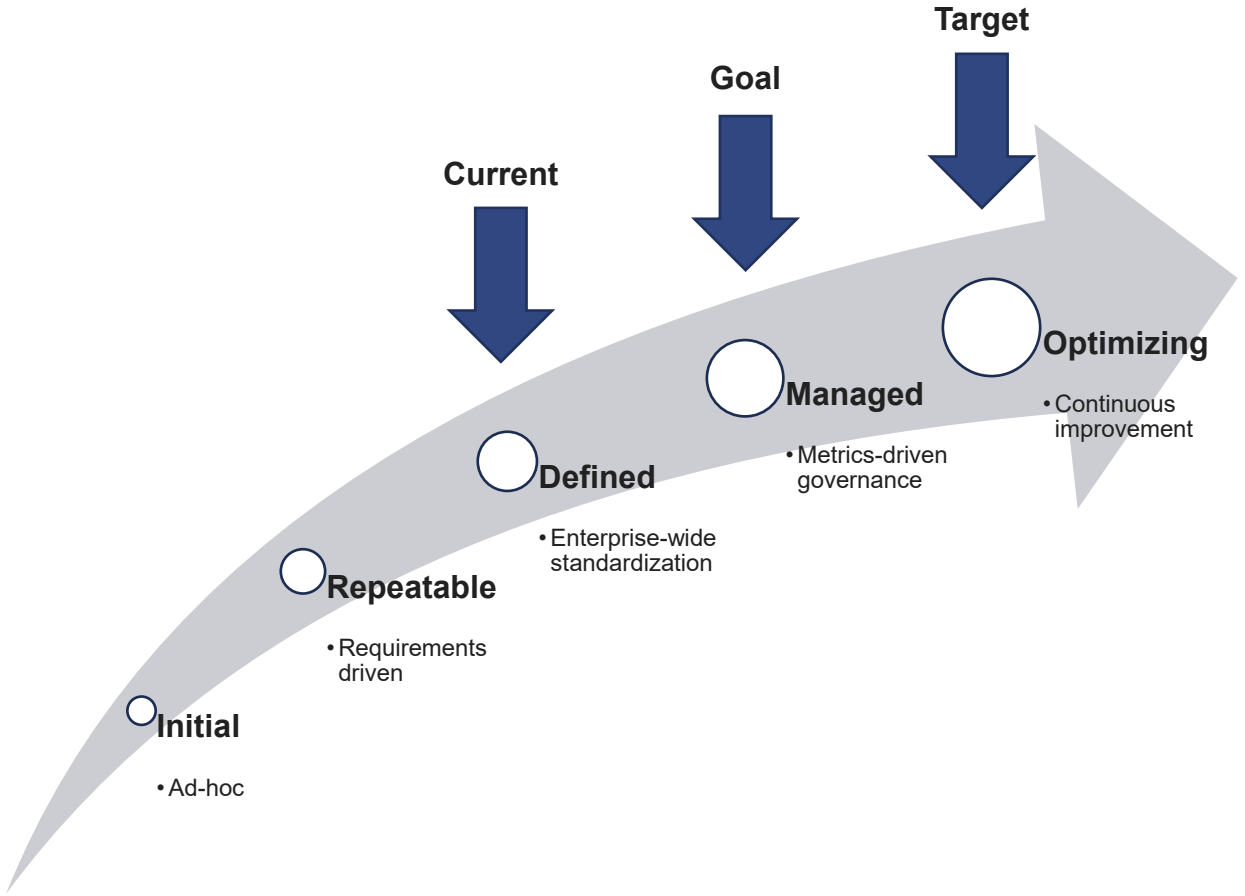
1. **Determine ECS role** in a distributed compliance model
2. Provide oversight, monitoring, testing, and/or ownership of conflicts of interest
3. **Build standardized oversight** and approach to distributed compliance functions
4. Access to branch systems and data
5. **Establish ownership** of compliance-related 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 ECS-specific professional development program
11. Obtain **resources** for expanded roles



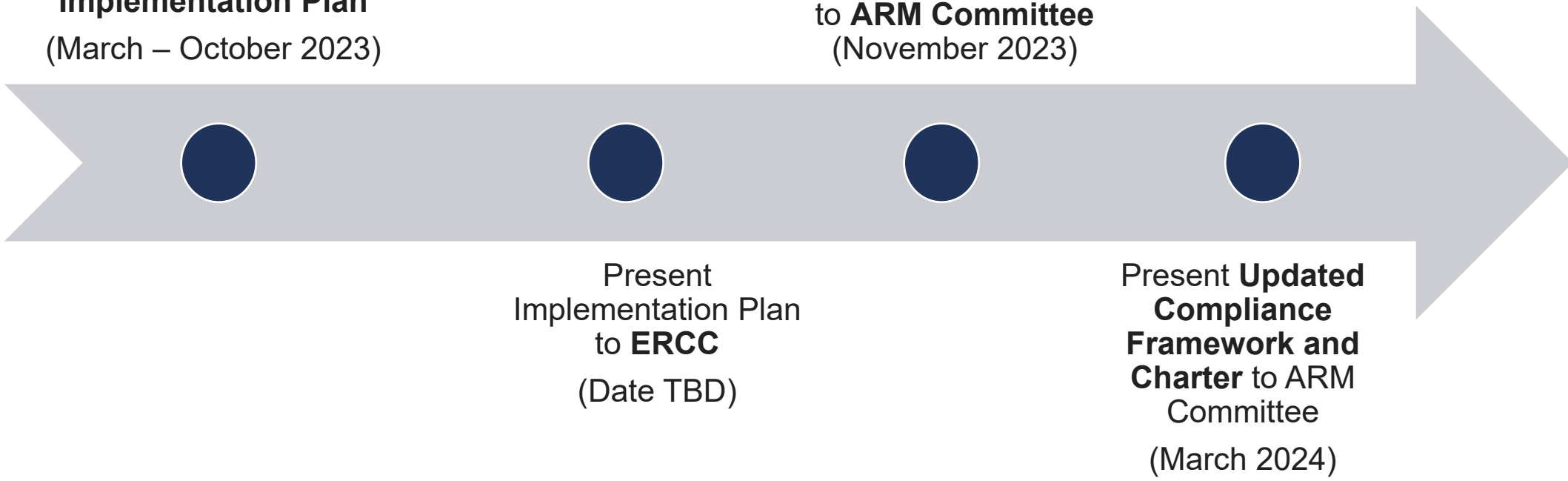
Recommendations: ERM

Enterprise Risk Management

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 analytics and **automation tools**
7. Automate risk data collection and reporting
8. Implement ERM-specific professional development program



Next steps


Develop Enterprise Risk and Compliance **Maturity Implementation Plan**
(March – October 2023)
Present Implementation Plan to **ERCC**
(Date TBD)
Present Implementation Plan to **ARM Committee**
(November 2023)
Present **Updated Compliance Framework and Charter** to ARM Committee
(March 2024)