RISK MANAGEMENT

Practical Plans for Implementing the

COSO ERM Model

GTE

Tallahassee AGA
Government Training Event

Agenda

01. ERM Overview

02. COSO ERM Framework

03. ERM - Strategy

04. ERM - Performance

05. Implementing ERM – Best Practices

06. FAMU's ERM Journey

"

If you don't invest in risk management, it doesn't matter what business you're in, it's a risky business.

- Gary Cohn

What is enterprise risk management?

Enterprise Risk Management (ERM) is defined by the Committee of Sponsoring Organizations (COSO) as "a **process**, effected by an entity's board of directors, management and other personnel, applied in **strategy-setting** and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide **reasonable assurance** regarding the achievement of **entity objectives**."
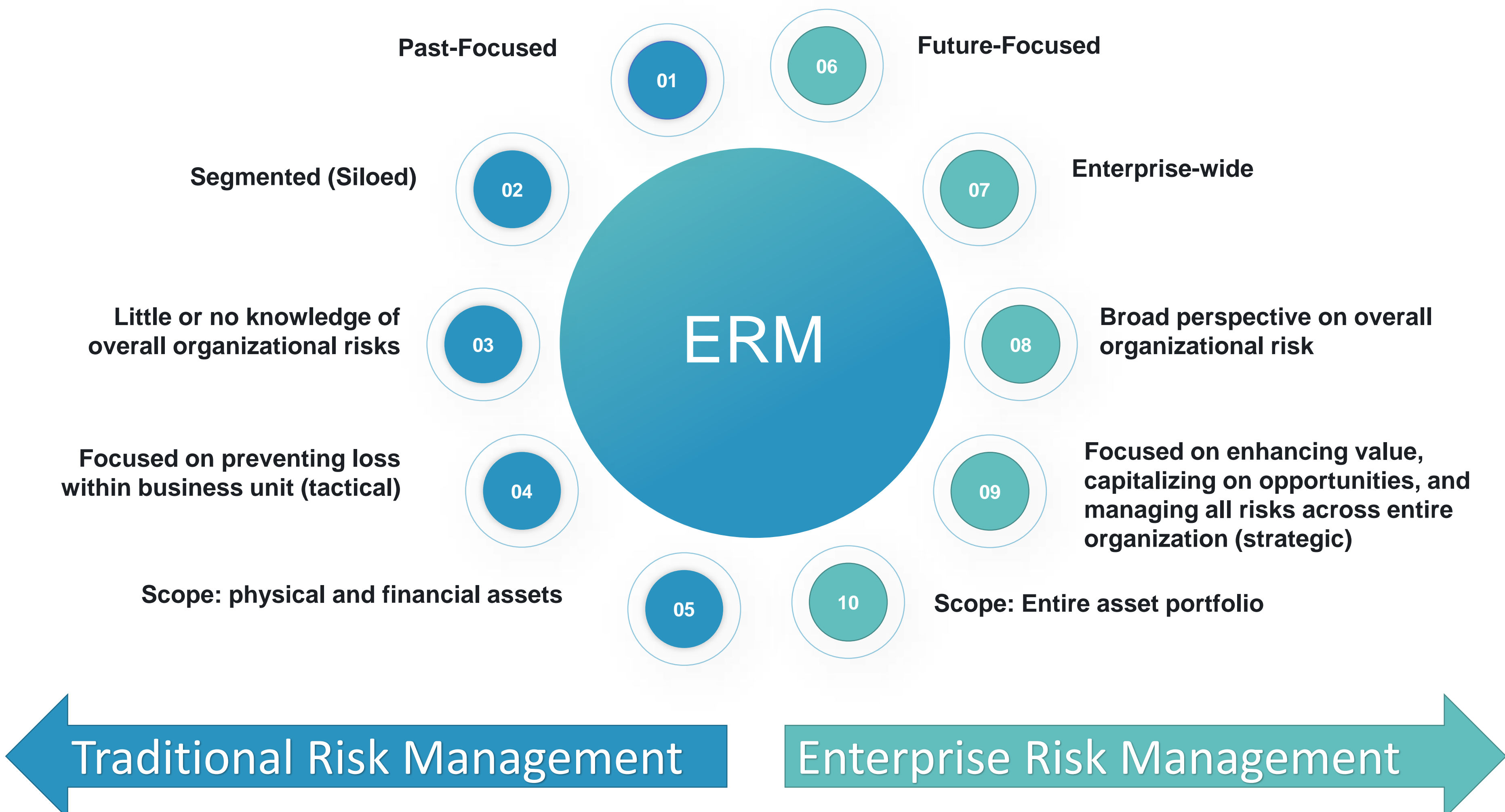
Basic Elements of ERM?
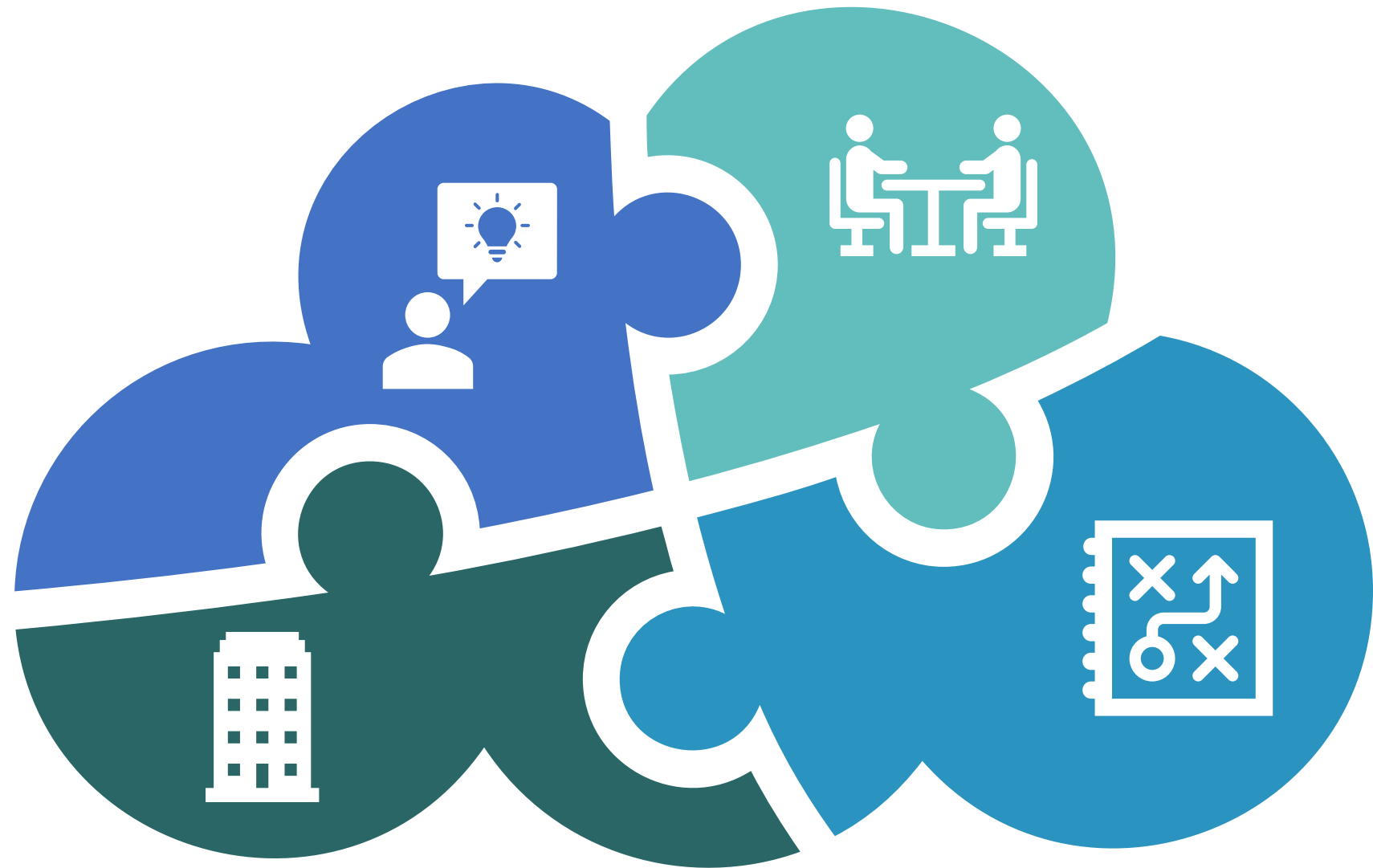
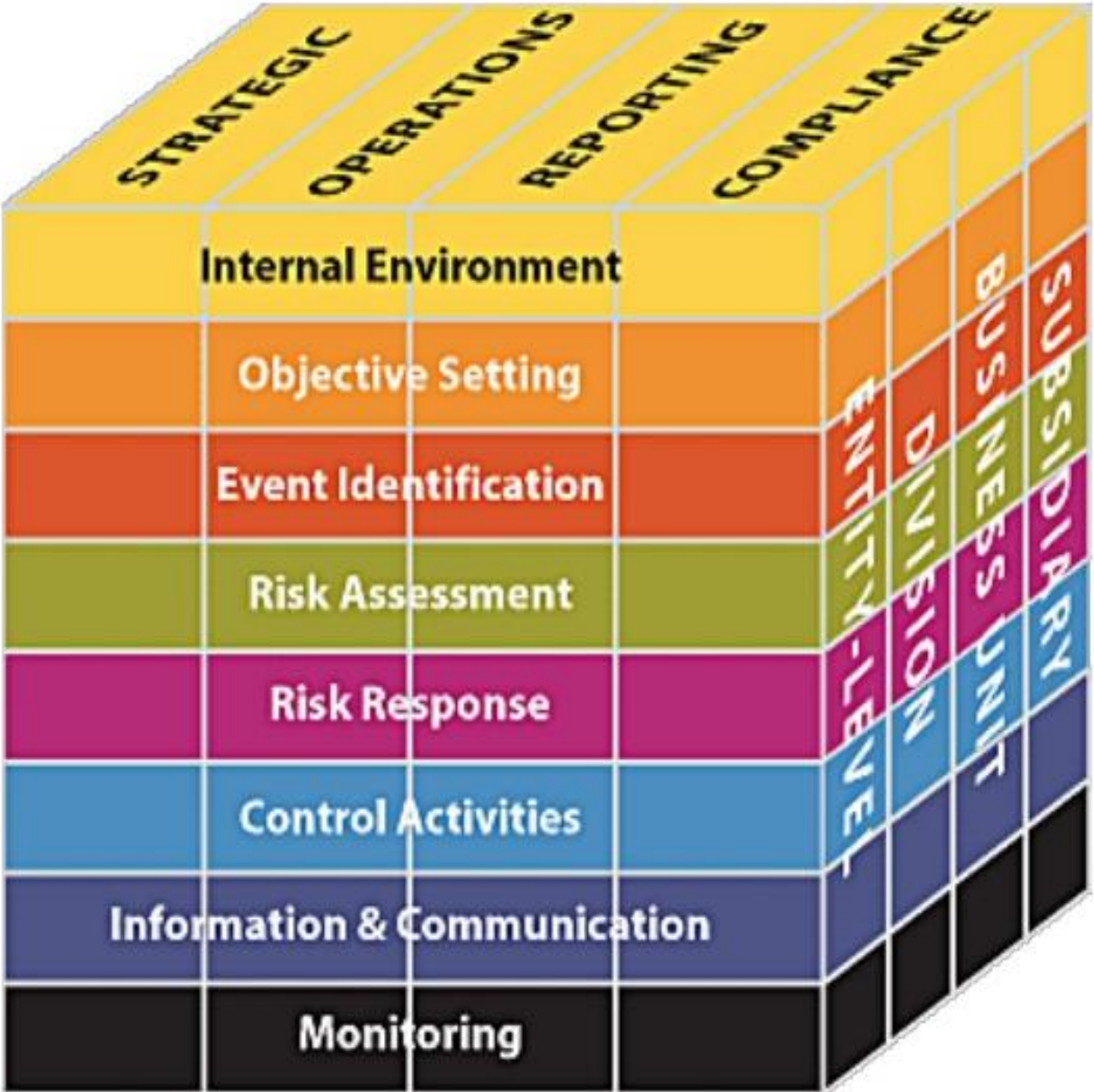Reframes Risk as Uncertainty

Proactive and Collaborative Process

Tied to Strategic Planning, Performance Management & Business Objectives

Focuses on Organizational Risks & Opportunities

Past-Focused

01

Future-Focused

06

Segmented (Siloed)

02

Enterprise-wide

07

Little or no knowledge of overall organizational risks

03

Broad perspective on overall organizational risk

08

Focused on preventing loss within business unit (tactical)

04

Focused on enhancing value, capitalizing on opportunities, and managing all risks across entire organization (strategic)

09

Scope: physical and financial assets

05

Scope: Entire asset portfolio

10

ERM

Traditional Risk Management

Enterprise Risk Management

# COSO ERM Model - 2004

Source: *Enterprise Risk Management – Integrated Framework: Executive Summary,*
Committee of Sponsoring Organizations of the Treadway Commission, September 2004, p. 5

Enterprise Risk Management Framework

Key Principles and Concepts

Common Risk Language

Clear Direction and Guidance

COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management
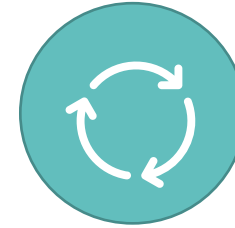Integrating with Strategy and Performance
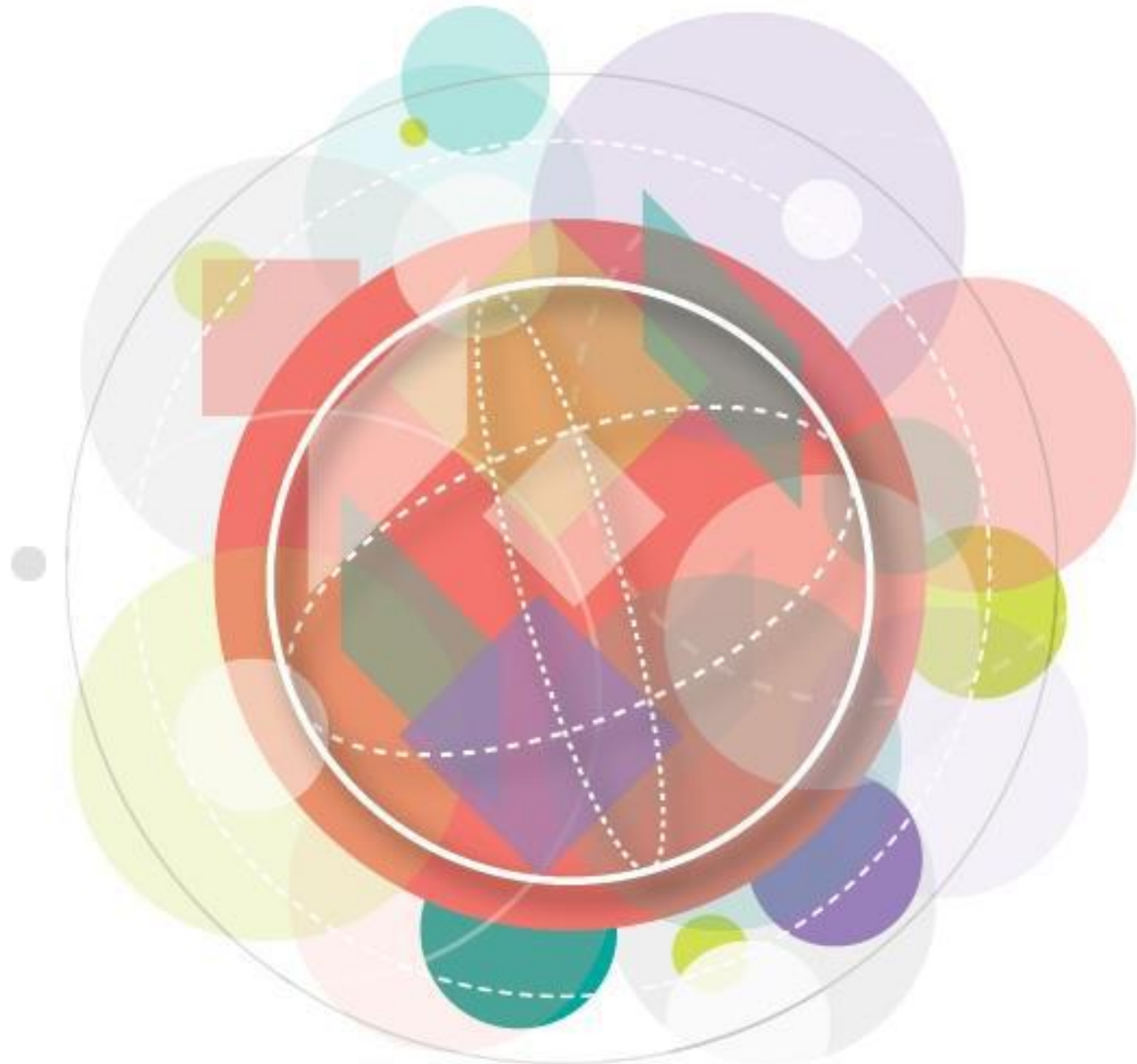
June 2017

Volume I

Provides greater insight into value of ERM

Enhances alignment between performance and ERM

Accommodates expectations for governance and oversight

Global common, tailored approach

View risk to setting and achieving objectives

Expands reporting for greater stakeholder transparency

Accommodates evolving technologies

Sets out core definitions, components and principles

Clarifies the importance of ERM in strategic planning and embedding it throughout an organization

Introduces 20 ERM Principles

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

ERM Impacts on Strategy

Risk the organization is willing to accept when setting strategy

Reveal non-alignment of strategy and business objectives

Potential risk exposure for the organization

Acceptance of inherent risk to achieve value

ERM Impacts on Performance

01

Risk Appetite

Understand the level of performance in the context of the entity's
risk appetite.

02

Optimal Performance

Find the optimal level of performance given the organization's
ability to manage risk.

03

Risk Tolerance
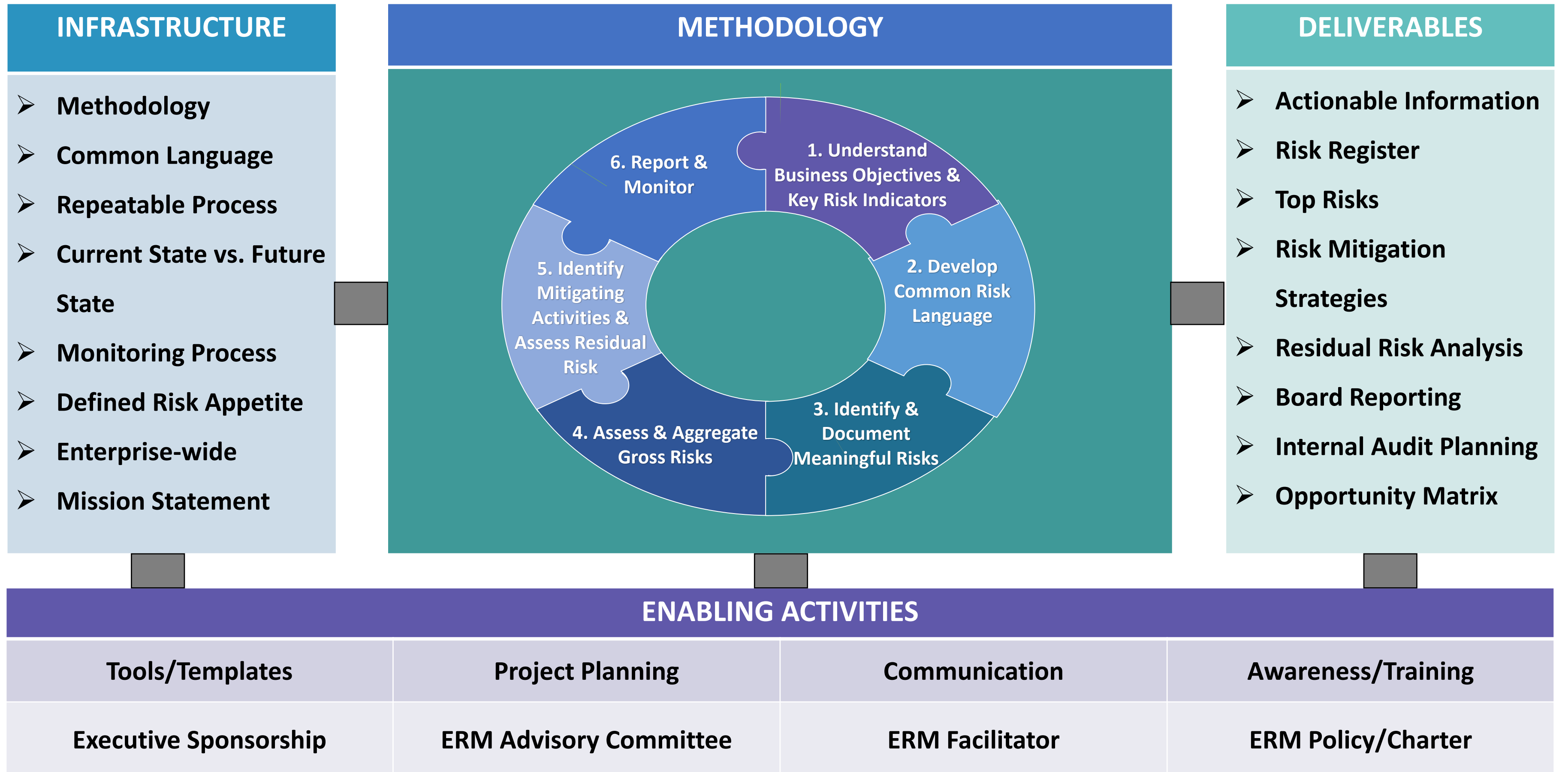
Determine the tolerance for variation in performance related to the target.

04

Risk Targets

Assess the potential impact of risk on predetermined targets.

Practical Approach to ERM

INFRASTRUCTURE

➤ Methodology

➤ Common Language

➤ Repeatable Process

➤ Current State vs. Future State

➤ Monitoring Process

➤ Defined Risk Appetite

➤ Enterprise-wide

➤ Mission Statement

METHODOLOGY

- 6. Report & Monitor
- 1. Understand Business Objectives & Key Risk Indicators
- 5. Identify Mitigating Activities & Assess Residual Risk
- 2. Develop Common Risk Language
- 4. Assess & Aggregate Gross Risks
- 3. Identify & Document Meaningful Risks

DELIVERABLES

➤ Actionable Information

➤ Risk Register

➤ Top Risks

➤ Risk Mitigation Strategies

➤ Residual Risk Analysis

➤ Board Reporting

➤ Internal Audit Planning

➤ Opportunity Matrix

ENABLING ACTIVITIES

Tools/Templates	Project Planning	Communication	Awareness/Training
Executive Sponsorship	ERM Advisory Committee	ERM Facilitator	ERM Policy/Charter

FAMU
DIVISION OF AUDIT
FLORIDA AGRICULTURAL AND MECHANICAL UNIVERSITY

ERM Program

Mission Statement

To provide meaningful, actionable, and timely strategic and performance risk intelligence to our stakeholders to enhance decision making and resource alignment while appropriately balancing risk and opportunity.

Vision Statement

The FAMU ERM program strives to become a thought leader in enterprise risk management practices through development of innovative and cost-effective methodologies that integrates enterprise risk management practices into the culture and strategic decision-making processes of academic, student, and administrative functions within educational institutions.

Strategic Plan Alignment

Strengthen the University's culture of strategic decision making through promotion and enhancement of enterprise risk management practices with an emphasis on engagement, education, reporting and accountability.

Timeline of ERM Program Implementation
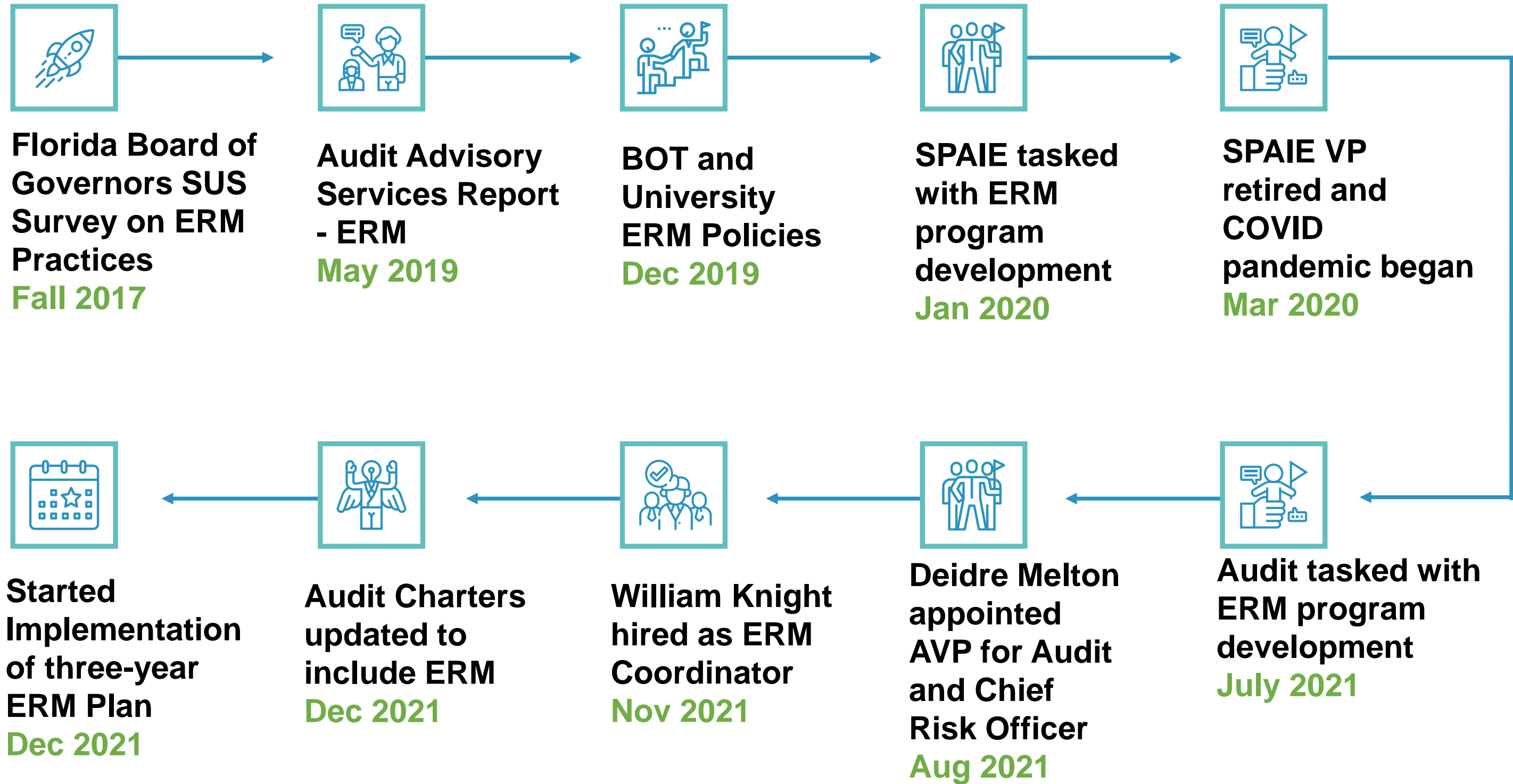
Florida Board of Governors SUS Survey on ERM Practices
Fall 2017

Audit Advisory Services Report - ERM
May 2019

BOT and University ERM Policies
Dec 2019

SPAIE tasked with ERM program development
Jan 2020

SPAIE VP retired and COVID pandemic began
Mar 2020

Started Implementation of three-year ERM Plan
Dec 2021

Audit Charters updated to include ERM
Dec 2021

William Knight hired as ERM Coordinator
Nov 2021

Deidre Melton appointed AVP for Audit and Chief Risk Officer
Aug 2021

Audit tasked with ERM program development
July 2021

FAMU ERM Policy

FLORIDA A&M UNIVERSITY
FLORIDA AGRICULTURAL AND MECHANICAL UNIVERSITY

University Policy Number: UP-01-02	Effective/Revision Date: December 3, 2019
Subject	Internal Controls and Enterprise Risk Management
Authority	Section 7(c), Article IX, Florida Constitution; Section 1010.01(5), Florida Statutes; BOT 2019-01
Applicability	This policy applies to all University units and employees.
Related	

I. POLICY PURPOSE AND INTENT

A. This policy is intended to improve mission delivery, reduce costs, and focus corrective actions toward key risks through the modernization of existing efforts by requiring the implementation an Enterprise Risk Management (ERM) capability coordinated with the strategic planning and strategic review process, and the internal controls processes.

II. STATEMENT OF POLICY

A. The Board of Trustees (BOT) has directed the University to modernize existing efforts by requiring the implementation of an Enterprise Risk Management (ERM) capability coordinated with the strategic planning and strategic review process, and the internal controls processes championed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in its publications Internal Controls - Integrated Framework and Enterprise Risk Management - Integrating with Strategy and Performance.
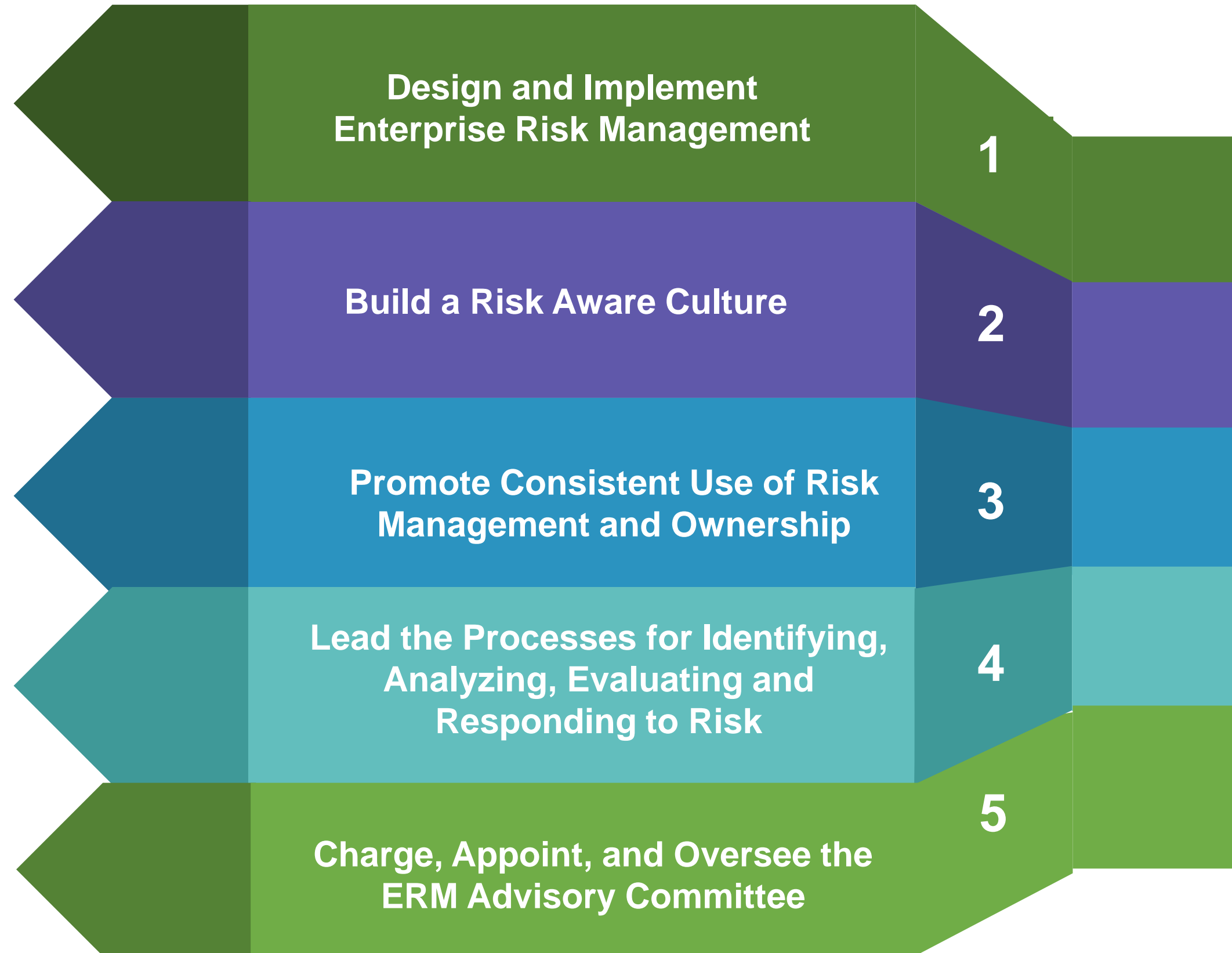
B. Successful implementation of this policy requires University leadership to establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame. An open and transparent culture results in the earlier identification of risks and allows the opportunity to develop a collaborative response, ultimately leading to more resilient operations.

- ➢ Requires FAMU to Implement COSO ERM
- ➢ Annual Risk Profile – Aligned with Strategy and Performance
- ➢ Risk Identification – New and Emerging or Changing Risks
- ➢ Establish an ERM Advisory Committee
- ➢ Risk Response Plans
- ➢ Progress Reports to BOT AACC
- ➢ Establish Chief Risk Officer Position
- ➢ Risk-aware Culture
- ➢ Roles and Responsibilities
  - Legal
  - Compliance & Ethics
  - Division of Audit
  - Senior Management
  - Employees

Chief Risk Officer: Roles and Responsibilities

FAMU [DIVISION OF AUDIT]
FLORIDA AGRICULTURAL AND MECHANICAL UNIVERSITY

Deidre Melton
AVP for Audit/
Chief Risk Officer

Design and Implement Enterprise Risk Management 1

Build a Risk Aware Culture 2

Promote Consistent Use of Risk Management and Ownership 3

Lead the Processes for Identifying, Analyzing, Evaluating and Responding to Risk 4

Charge, Appoint, and Oversee the ERM Advisory Committee 5

Year 1: ERM Program Implementation

FAMU [DIVISION OF AUDIT]
FLORIDA AGRICULTURAL AND MECHANICAL UNIVERSITY

Networking & Research

Build a network of ERM professionals within the educational industry and research tools and best practices

Governance

Develop or facilitate the development of risk charters, risk appetite statement, and ERM handbook

ERM Committee

Develop a cross-functional, inclusive, and engaged ERM Advisory Committee

Tools

Develop tools for identifying, assessing, responding to, monitoring, and reporting risks. Develop risk decision making tools.

Strategic Plan Alignment

Work with the strategic planning committee to identify and prioritize risks to the strategic plan currently under development.

ERM Program Plan for Year 2

FAMU [DIVISION OF **AUDIT**]
FLORIDA AGRICULTURAL AND MECHANICAL UNIVERSITY

Strategic Plan
Identify and prioritize risks to the strategic plan. Identify risk owners and monitoring process of KRIs and KPIs.

Training
Develop different modes of ERM training for the campus community and stakeholders

Budget Integration
Work with budget council to integrate risk management information into budget decision making process.

Risk Profile
Develop the University full risk profile and present to senior leadership and the Board of Trustees

ERM Implementation Challenges

Organizational Placement

Identifying ERM Program Leader

Identifying Risk Champions

Demonstrating Program Value

Understanding Risk Assessment Practices vs Risk Management

Assigning Risk Ownership

Allocation of Resources for ERM

Educating Staff and Management

Defining Risk Appetite

Establishing Risk Tolerance Levels

Internal Audit's Skills for ERM

- Awareness
- Have Access
- Audit Charter
- Established Relationships
- Understand Standard Tools
- Facilitation Skills
- Risks & Controls
- Reporting

Internal Audit Role in Risk Management

CORE INTERNAL AUDIT ROLES WITH REGARD TO ERM	LEGITIMATE INTERNAL AUDIT ROLES WITH SAFEGUARDS	ROLES INTERNAL AUDITING SHOULD NOT UNDERTAKE

Audit	CRO	Management
➢ Provide assurance that risks are correctly stated and evaluated ➢ Provide assurance that mitigating actions are operating ➢ Evaluate risk management processes ➢ Evaluate reporting and management of key risks	➢ Facilitate identification and evaluation of risks ➢ Coach management in risk response ➢ Coordinate ERM activities ➢ Consolidate reporting on risks ➢ Maintain and develop ERM frameworks ➢ Champion establishment of ERM ➢ Develop ERM strategy for board approval	➢ Set the risk appetite ➢ Impose risk management processes ➢ Manage risk ➢ Make decisions and implement risk responses ➢ Implement mitigating actions for risks ➢ Accountable for risk management

Source: Adapted from "Position Statement: The Role of Internal Auditing in Enterprise-wide Risk Management"

Key ERM Reminders

Each organization needs a tailored approach

ERM is not a compliance exercise

ERM is a mindset

ERM facilitates information sharing

ERM facilitates decision making

Resources

01 [Enterprise Risk Management – Integrating with Strategy and Performance (2017)](#)

02 [Creating and Protecting Value – Understanding and Implementing Enterprise Risk Management](#)

03 [Risk Appetite – Critical to Success: Using Risk Appetite to Thrive in a Changing World (2020)](#)

04 [FAMU Division of Audit Advisory Services Report – Enterprise Risk Management](#)

05 [FAMU University Policy UP-01-02: Internal Controls and Enterprise Risk Management](#)

06 [IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management](#)