

**FAMU**

DIVISION OF  
**AUDIT**

FLORIDA AGRICULTURAL AND MECHANICAL UNIVERSITY



**FAMU Management Seminar  
Enterprise Risk Management  
April 7, 2021**

# Agenda



**What is Risk?**

**What is ERM?**

**ERM in Higher Ed**

**FAMU Risk Management & ERM**

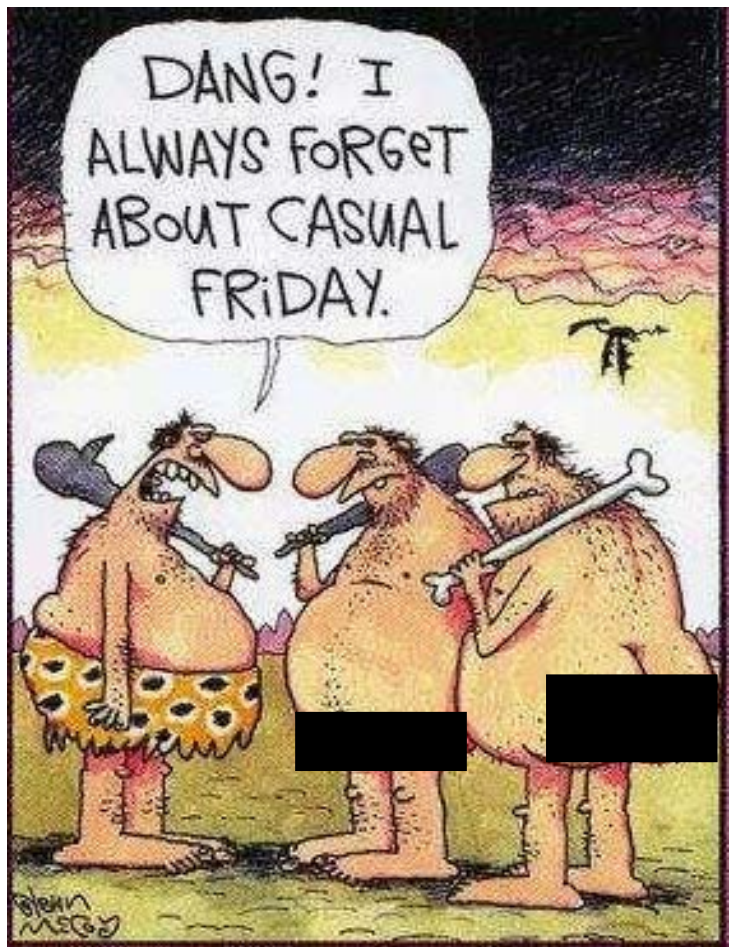
**COSO ERM Framework**

**ERM Challenges & Reminders**

**Q&A**



Risk: As Old As Time



# Reputational Risk

# Risk

Risk is the probability that an event will occur and adversely affect the achievement of objectives.



# ERM Milestones

YEAR	MILESTONE
1900s	Risk Management: Logical, disciplined approach to future uncertainties
1974	Gustave Hamilton Risk Management Circle
1987	COSO: Report on Fraudulent Financial Reporting
1992	COSO: Internal Controls: Integrated Framework Cadbury Report: Financial Aspect of Corporate Governance CoCo: Canadian Institute of Chartered Accountant's Criteria for Control Framework
1993	Chief Risk Officer
1995	First Risk Management Standard: AS/NZS 4360
1996	COBIT: IT Governance
1999	GAO: Standards for Internal Control in Federal Government
2004	COSO: ERM – Integrated Framework
2009	ISO 31000: Suite of Risk Management Standards
2016	OMB: Circular A-123 requires Federal Agencies to implement ERM and Internal Controls
2017	COSO: ERM – Integrating with Strategy and Performance

# Enterprise Risk Management

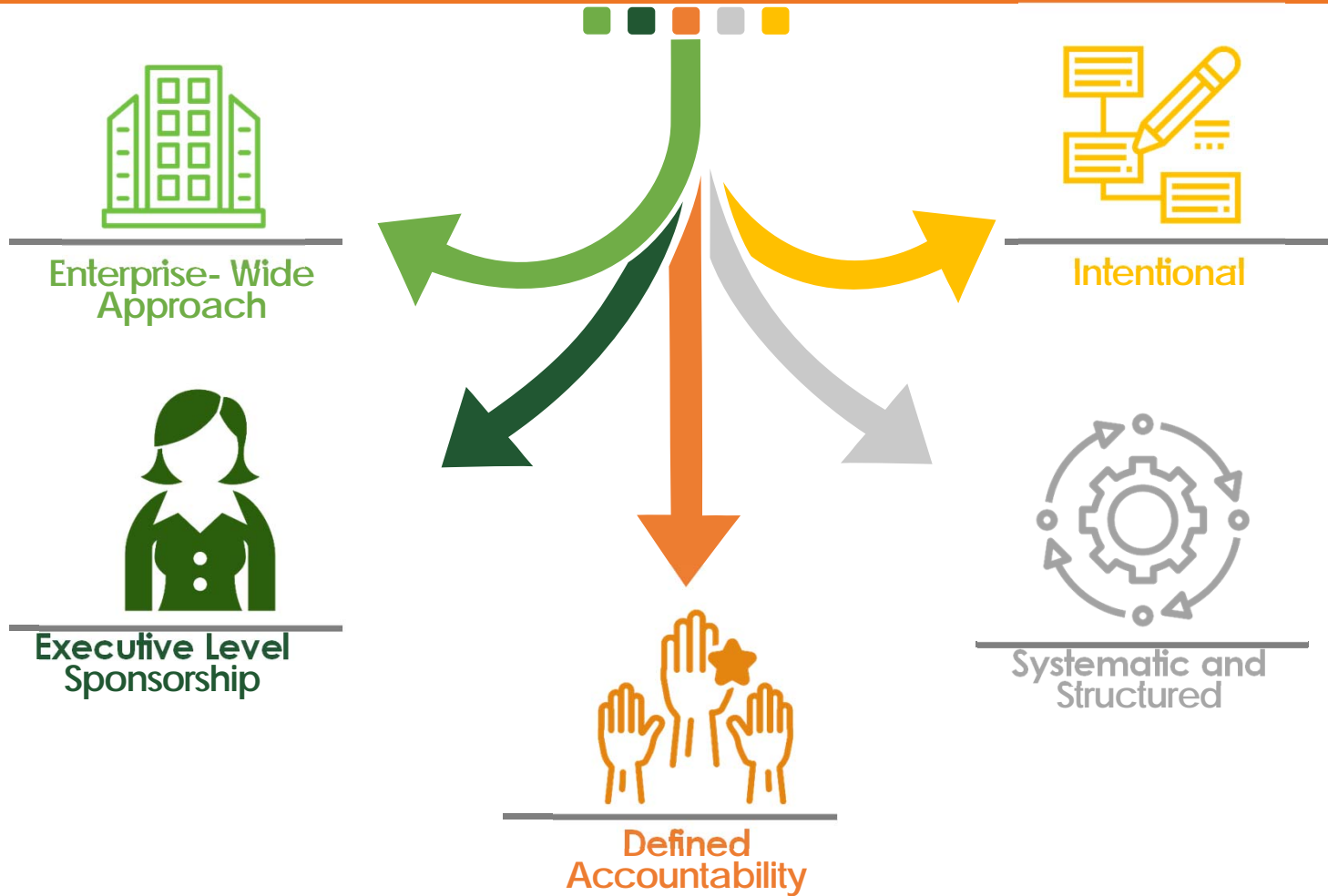


Enterprise Risk Management (ERM) is defined by the Committee of Sponsoring Organizations (COSO) as “a **process**, effected by an entity’s board of directors, management and other personnel, applied in **strategy-setting** and across the enterprise, designed to identify potential events that may affect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

# Risk Management V. ERM

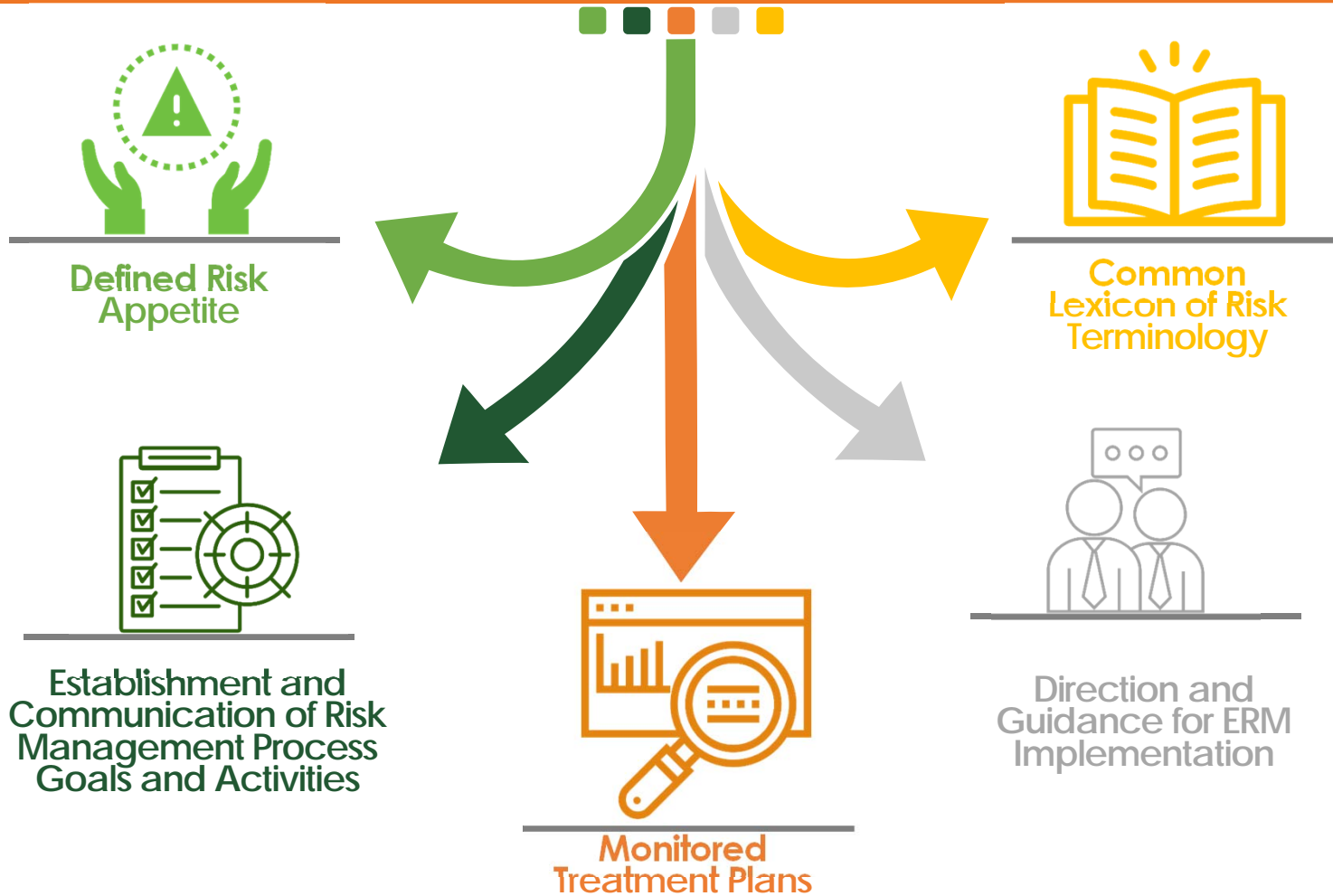
Traditional Risk Management	Enterprise Risk Management
Past-focused	Future-focused
Segmented/Siloed	Enterprise-wide
Little or no knowledge of overall organizational risks	Broad perspective on overall organizational risk
Focused on preventing loss within business unit (tactical)	Focused on enhancing value, capitalizing on opportunities, and managing all risks across entire organization (strategic)
Scope: physical and financial assets	Scope: entire asset portfolio
Siloed risk mitigation	Enterprise-wide risk mitigation

# ERM Program Characteristics





# ERM Program Characteristics




# ERM Program Value



**The biggest value in ERM frameworks lies in their promotion of continuous improvement, diligent management practices, and ongoing monitoring.**

# Common ERM Misconceptions

## ERM is . . .

- A continuous Process
  - A Part of Routine Business Processes
  - Linked to Strategic Goals and Objectives
  - A Means to Hold Leadership Accountable
  - A Way to Identify and manage Current and Emerging Risks
- 

## ERM is not . . .

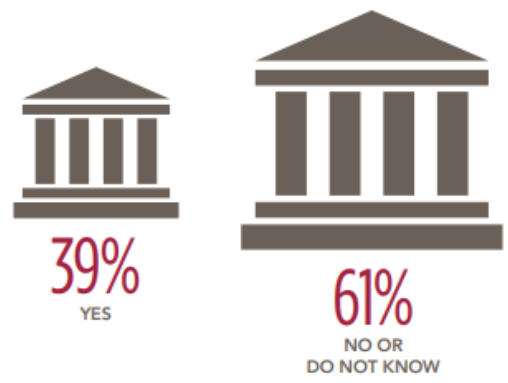
- A One-time Process
  - A Tool or Software
  - A One-size fits all Framework
  - A Means to Prevent All Risks
  - A Means to Avoid All Risks
  - A Method to Manage Individual Risks
- 

# ERM in Higher Ed

## A Wake-up Call: Enterprise Risk Management at Colleges and Universities Today

A Survey by the Association of Governing Boards  
 of Universities and Colleges and  
 United Educators

Percent of respondents who say their  
 institution has conducted an ERM process  
 in the last two years:





## Three Keys to a Successful ERM Program

### 1. Get leadership Buy-in

- Formal Ownership
- Cross-functional Coordination
- Visibility to President and Board

### 2. Act

- 20% Planning – Organize, Identify, Assess
- 80% Acting – Risk Treatment and Implementation

### 3. Manage Burnout

- Process v. Project
- Matures Over Time

## Three Keys to a Successful ERM Program



### Get Leadership Buy-In

- Formal Ownership
- Cross-functional Coordination
- Visibility to President and Board



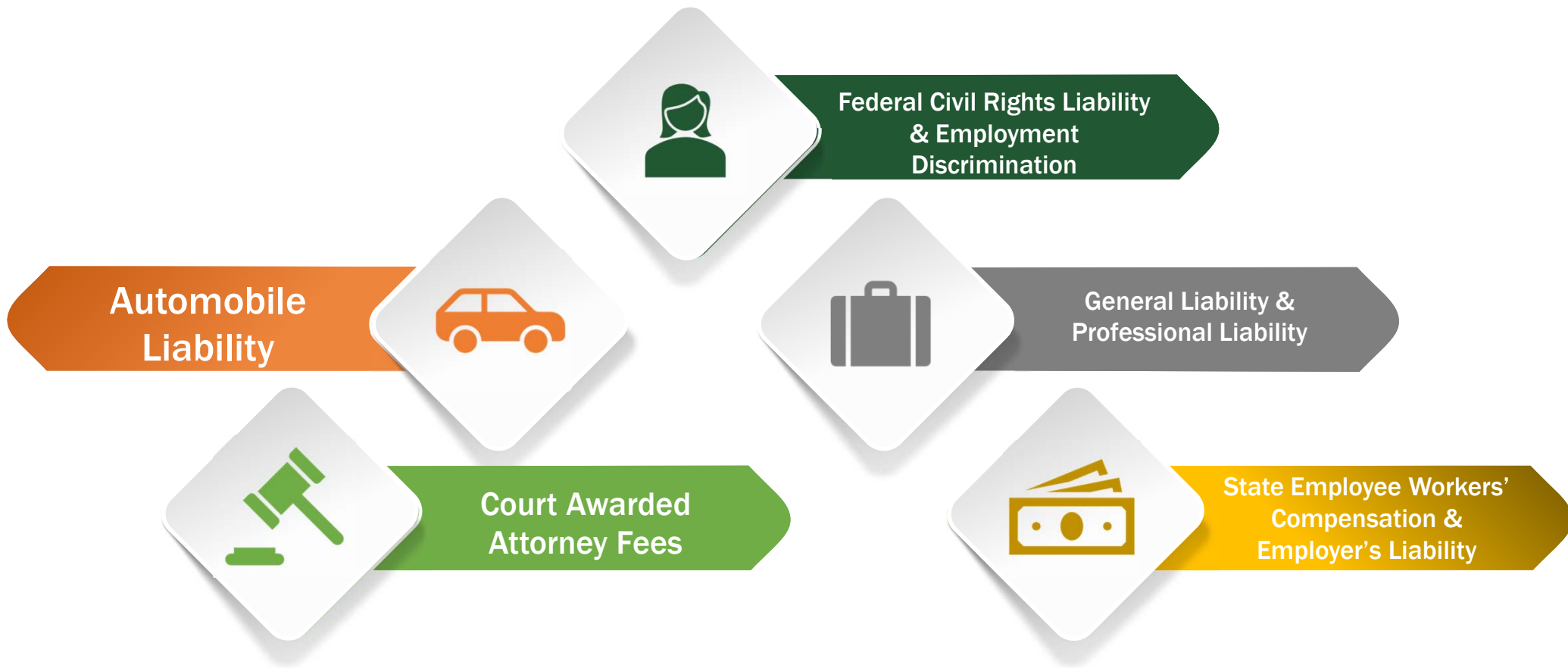
### Act

- 20% Planning – Organize, Identify, Assess
- 80% Acting – Risk Treatment and Implementation



### Manage Burnout

- Process v. Project
- Matures Over Time



# FAMU ERM Policy



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

**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



# COSO

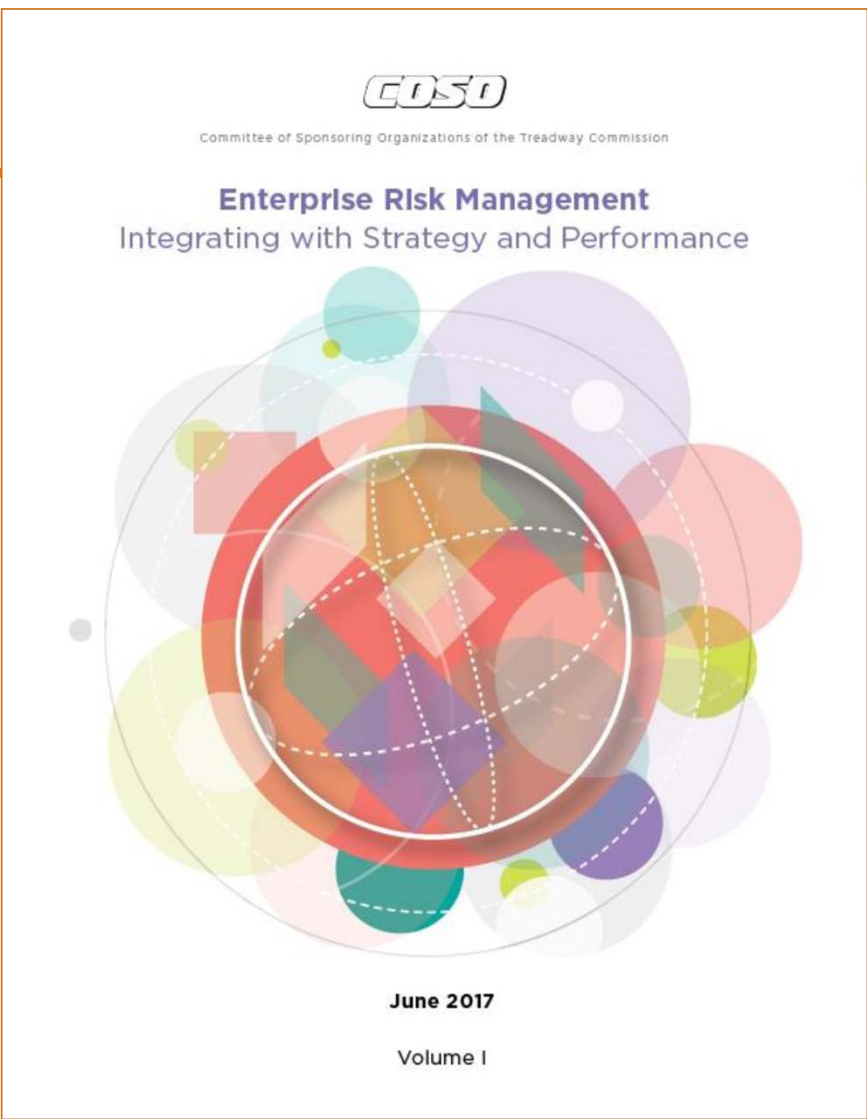


> 600,000  
professionals

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence.

*Enterprise Risk Management Framework: Integrating with Strategy and Performance (June 2017)*

Enterprise Risk Management Framework: Integrating with Strategy and Performance © 2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.



# 1. Document Structure

- Framework focused on fewer components (five)
- Uses focused call-out examples to emphasize key points



- Follows the business model versus isolated risk management process

## 2. Introduces Principles





# Governance & Culture



1. **Exercises Board Risk Oversight** - Board of directors provides oversight of strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Operating Structures** - Organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Culture** - Organization defines desired behaviors that characterize entity's desired culture.
4. **Demonstrates Commitment to Core Values** - Organization demonstrates commitment to entity's core values.
5. **Attracts, Develops, and Retains Capable Individuals** - Organization committed to building human capital in alignment with strategy and business objectives.

# Strategy & Objective-Setting



6. **Analyzes Business Context** - Organization considers potential effects of business context on risk profile.
7. **Defines Risk Appetite** - Organization defines risk appetite in context of creating, preserving, and realizing value.
8. **Evaluates Alternative Strategies** - Organization evaluates alternative strategies and potential impact on risk profile.
9. **Formulates Business Objectives** - Organization considers risk while establishing business objectives at various levels that align and support strategy.



- 10. Identifies Risk** - Organization identifies risk that impacts performance of strategy and business objectives.
- 11. Assesses Severity of Risk** - Organization assesses risk severity.
- 12. Prioritizes Risks** - organization prioritizes risks as basis for selecting risk responses.
- 13. Implements Risk Responses** - Organization identifies and selects risk responses.
- 14. Develops Portfolio View** - Organization develops and evaluates portfolio view of risk.

# Review & Revision



- 15. Assesses Substantial Change** - Organization identifies and assesses changes that may substantially affect strategy and business objectives.
- 16. Reviews Risk and Performance** - Organization reviews entity performance and considers risk.
- 17. Pursues Improvement in Enterprise Risk Management** - Organization pursues improvement of enterprise risk management.



# Information, Communication, & Reporting



- 18. Leverages Information Systems** - Organization leverages entity's information and technology systems to support enterprise risk management.
- 19. Communicates Risk Information** - Organization uses communication channels to support enterprise risk management.
- 20. Reports on Risk, Culture, and Performance** - Organization reports on risk, culture, and performance at multiple levels and across entity.






### 3. Incorporates New Graphics

- Graphic has stronger ties to the business model



## 4. Focus on Integration

**Integrating ERM with business practices results in better information that supports improved decision-making and leads to enhanced performance. It helps organizations to:**

-  **Anticipate risks earlier or more explicitly, opening up more options for managing the risks**
-  **Identify and pursue existing and new opportunities**
-  **Respond to deviations in performance more quickly and consistently**
-  **Develop and report a more comprehensive and consistent portfolio view of risk**
-  **Improve collaboration, trust, and information-sharing**

# 5. Emphasizes Values

## Enhances Value Focus



**Create**

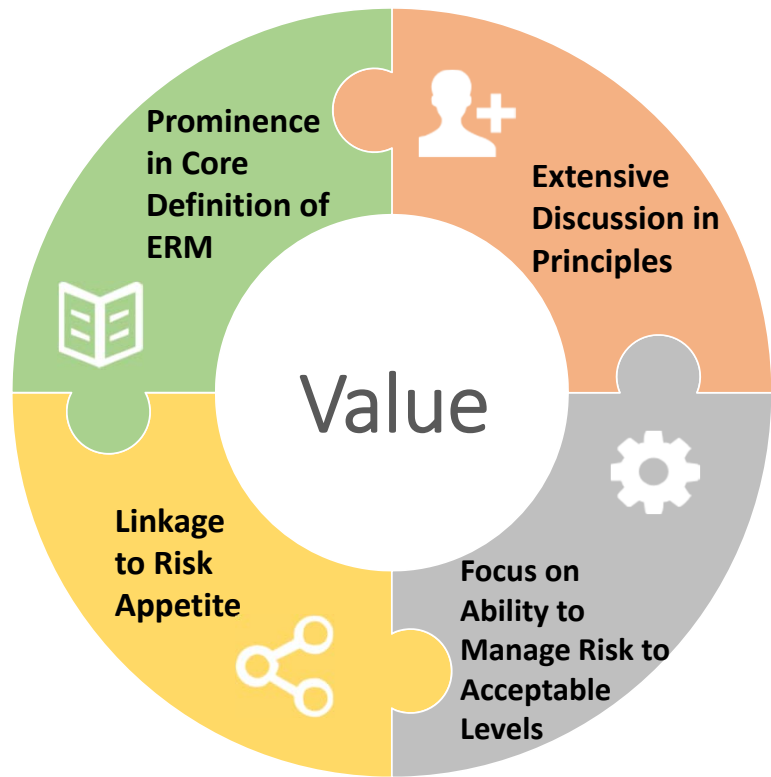


**Preserve**



**Realize**

## Embeds Value Throughout the Framework



# 6. Link to Strategy

Explores strategy from three perspectives:





# 7. Links to Performance

**ERM  
Links to  
Performance**



## Achievement of Strategy

Enables achievement of strategy by actively managing risk and performance



## Support Risk Identification

Exploring how enterprise risk management practices support risk identification and assessment that impact performance



## Tolerance

Discussing tolerance for variations in performance



## Risk Management Perspective

Manages risk in the context of achieving strategy and business objectives – not as individual risks



# 9. Focuses on Decision-making



Explores how enterprise risk management drives risk aware decision-making



Highlights how risk awareness optimizes and aligns decisions impacting performance

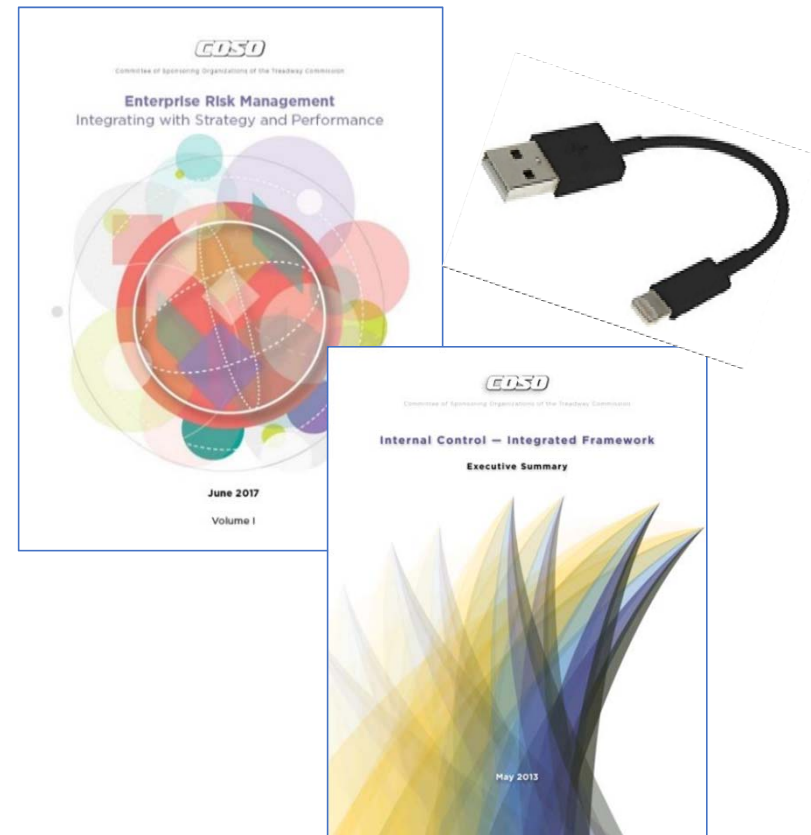


Explores how risk aware decisions affect risk profile



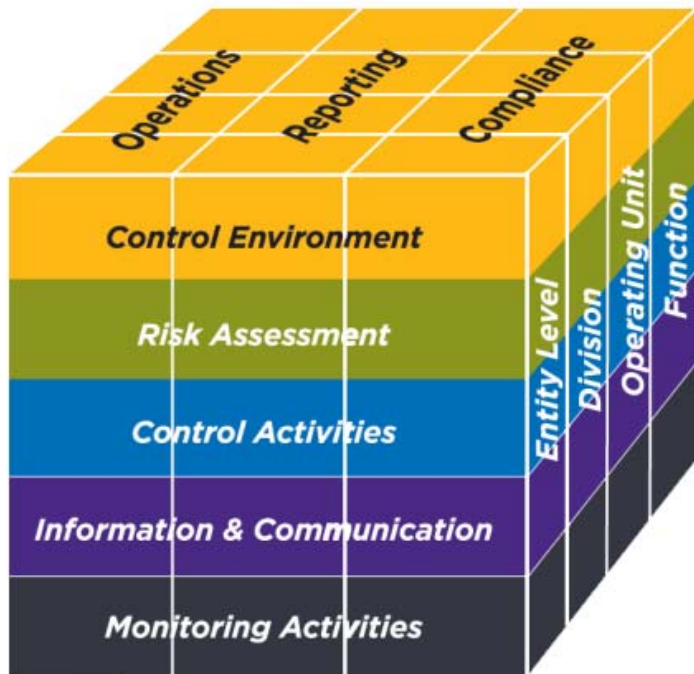
# 10. Link to Internal Controls

- 🔗 Document does not replace the *Internal Control – Integrated Framework*
- 🔗 The frameworks are distinct and complementary
- 🔗 Both use a components-and-principles structure
- 🔗 Aspects of internal control common to enterprise risk management are not repeated
- 🔗 Some aspects of internal control are developed further in this framework



# Tips: Learn and Implement the COSO Internal Control Integrated Framework

## COSO Cube

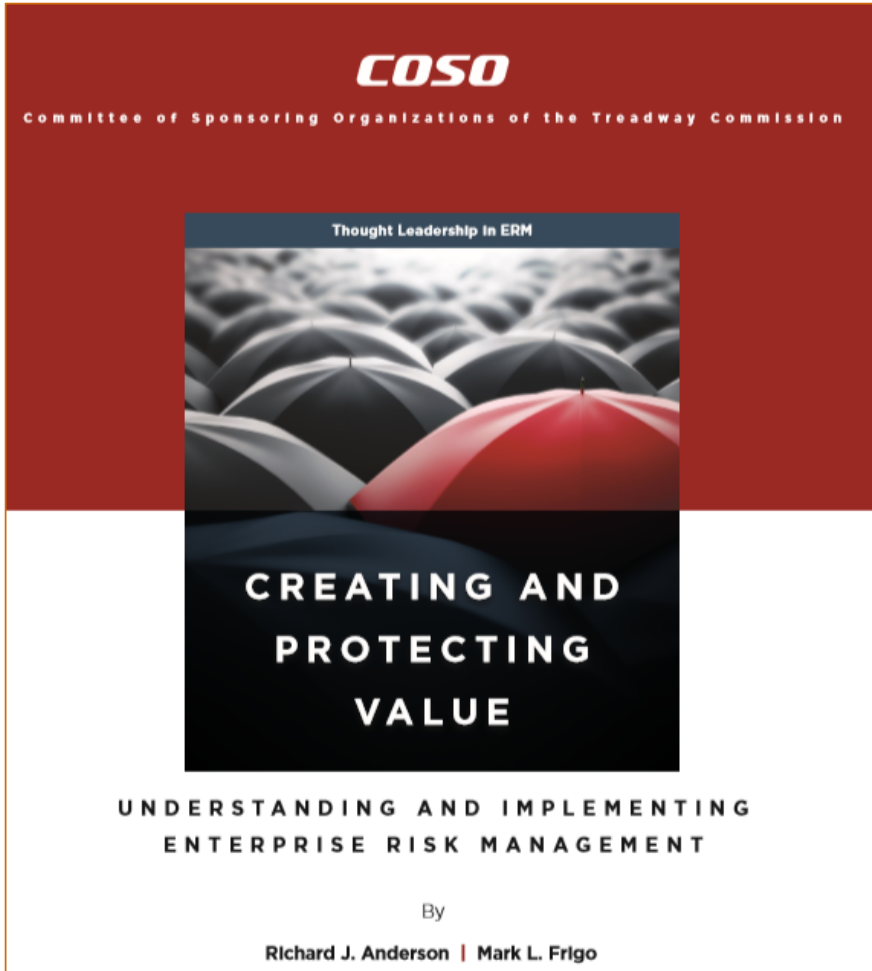


## 17 Principles of Control

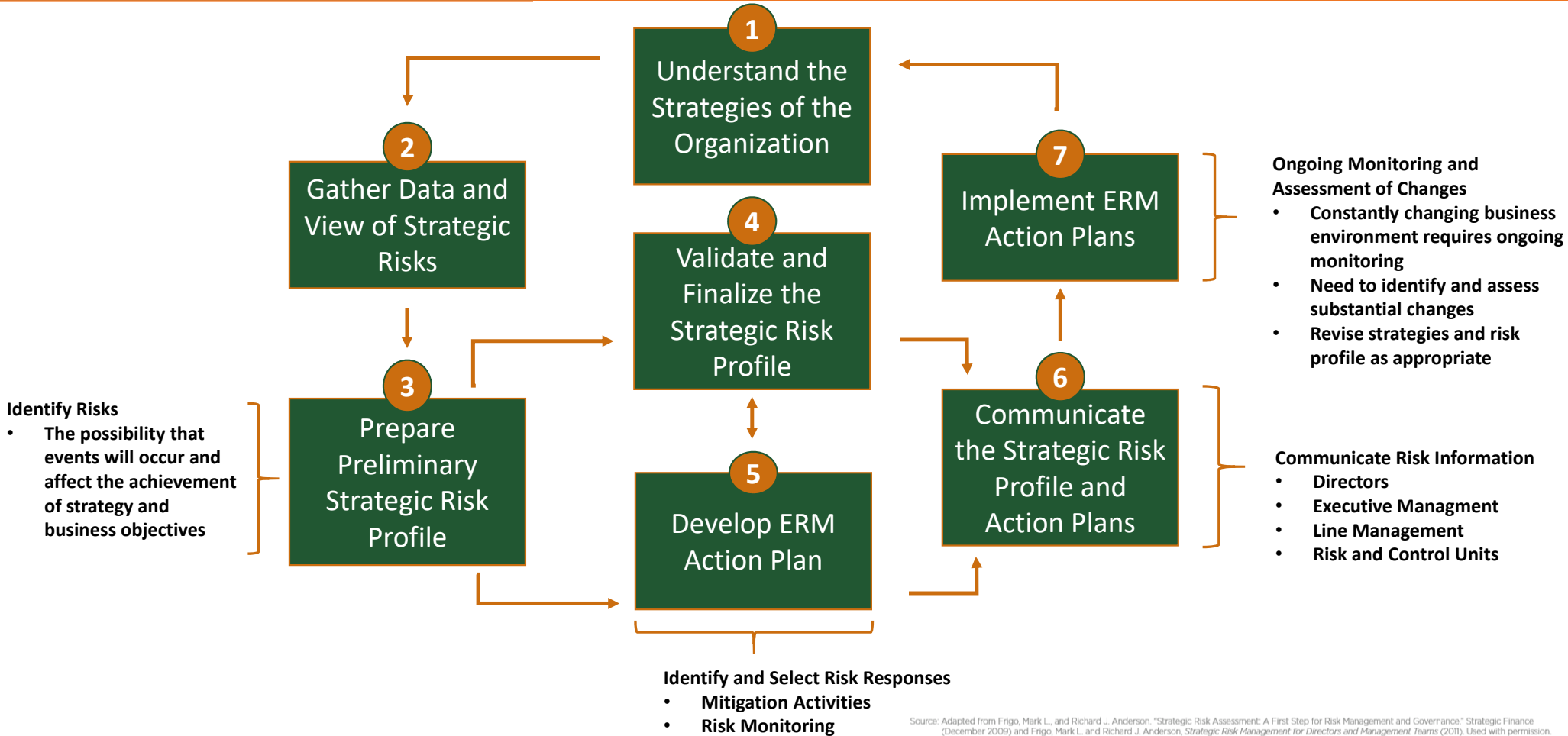
1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability
6. Specifies relevant objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures
13. Uses relevant information
14. Communicates internally
15. Communicates externally
16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Go to [www.coso.org](http://www.coso.org) or the Division of Audit website for more information on internal controls





# Risk Assessment Process



Source: Adapted from Frigo, Mark L., and Richard J. Anderson. "Strategic Risk Assessment: A First Step for Risk Management and Governance." *Strategic Finance* (December 2009) and Frigo, Mark L. and Richard J. Anderson, *Strategic Risk Management for Directors and Management Teams* (2011). Used with permission.

# ERM Challenges

➤ **ERM is too costly to implement!**



➤ **Current staff already have a huge workload!**



➤ **We don't have resources for ERM!**



➤ **How do staff know what risks they "own"?**



➤ **We already do risk assessment!**

# Key Reminders



**Each organization is unique.**



**ERM is a mindset**



**Each organization needs a tailored approach.**



**ERM facilitates information-sharing**



**ERM is not a compliance exercise.**



**ERM facilitates decision-making**



FLORIDA AGRICULTURAL AND MECHANICAL UNIVERSITY

## Questions



**Please send all questions and requests for further information to the Division of Audit:**  
**[auditandcompliance@famu.edu](mailto:auditandcompliance@famu.edu)**



FLORIDA AGRICULTURAL AND MECHANICAL UNIVERSITY

## Division of Audit Contacts



**Joseph Maleszewski**

VP of Audit

E: [joseph.Maleszewski@famuedu](mailto:joseph.Maleszewski@famuedu)

P: 850-412-7802



**Deidre Melton**

Director of Audit

E: [deidre.melton@famuedu](mailto:deidre.melton@famuedu)

P: 850-599-3131



Thank you!



# FLORIDA A&M UNIVERSITY

Founded in 1887 as the State Normal College for Colored Students, Florida Agricultural and Mechanical University (FAMU) is the only historically state supported educational facility for African Americans in Florida. It has always been co-educational. In 1890, the second Morrill Act was passed. This enabled the school to become the Black Land Grant College for the State of Florida. In 1891, the college was moved from its original location west of town to its present location which was once the site of "Highwood," Territorial Governor W.P. Duval's slave plantation. The site is one of the highest hills in Tallahassee. The school was known as Florida A&M College from 1909 until 1953 when it attained university status.