<table>
<thead>
<tr>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is Risk?</td>
</tr>
<tr>
<td>What is ERM?</td>
</tr>
<tr>
<td>ERM in Higher Ed</td>
</tr>
<tr>
<td>FAMU Risk Management &amp; ERM</td>
</tr>
<tr>
<td>COSO ERM Framework</td>
</tr>
<tr>
<td>ERM Challenges &amp; Reminders</td>
</tr>
<tr>
<td>Q&amp;A</td>
</tr>
</tbody>
</table>
Risk: As Old As Time

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

<table>
<thead>
<tr>
<th>YEAR</th>
<th>MILESTONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1900s</td>
<td>Risk Management: Logical, disciplined approach to future uncertainties</td>
</tr>
<tr>
<td>1974</td>
<td>Gustave Hamilton Risk Management Circle</td>
</tr>
</tbody>
</table>
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.”
<table>
<thead>
<tr>
<th>Traditional Risk Management</th>
<th>Enterprise Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past-focused</td>
<td>Future-focused</td>
</tr>
<tr>
<td>Segmented/Siloed</td>
<td>Enterprise-wide</td>
</tr>
<tr>
<td>Little or no knowledge of overall organizational risks</td>
<td>Broad perspective on overall organizational risk</td>
</tr>
<tr>
<td>Focused on preventing loss within business unit (tactical)</td>
<td>Focused on enhancing value, capitalizing on opportunities, and managing all risks across entire organization (strategic)</td>
</tr>
<tr>
<td>Scope: physical and financial assets</td>
<td>Scope: entire asset portfolio</td>
</tr>
<tr>
<td>Siloed risk mitigation</td>
<td>Enterprise-wide risk mitigation</td>
</tr>
</tbody>
</table>
ERM Program Characteristics

- Enterprise-Wide Approach
- Executive Level Sponsorship
- Intentional
- Systematic and Structured
- Defined Accountability
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
A Wake-up Call: Enterprise Risk Management at Colleges and Universities Today

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

- 39% YES
- 61% NO OR DO NOT KNOW

United Educators
National Association of College and University Business Officers

AGB Association of Governing Boards of Universities and Colleges
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

- 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

---

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

## 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 of 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.
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

<table>
<thead>
<tr>
<th>Governance &amp; Culture</th>
<th>Strategy &amp; Objective-Setting</th>
<th>Performance</th>
<th>Review &amp; Revision</th>
<th>Information, Communication, &amp; Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Attracts, Develops, and Retains Capable Individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

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.

7. **Defines Risk Appetite** - Organization defines risk appetite in context of creating, preserving, and realizing value.


9. **Formulates Business Objectives** - Organization considers risk while establishing business objectives at various levels that align and support strategy.


12. **Prioritizes Risks** - Organization prioritizes risks as basis for selecting risk responses.


15. **Assesses Substantial Change** - Organization identifies and assesses changes that may substantially affect strategy and business objectives.


17. **Pursues Improvement in Enterprise Risk Management** - Organization pursues improvement of enterprise risk management.
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

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.
5. Emphasizes Values

Enhances Value Focus

Create
Preserve
Realize

Embeds Value Throughout the Framework

Prominence in Core Definition of ERM
Extensive Discussion in Principles
Linkage to Risk Appetite
Focus on Ability to Manage Risk to Acceptable Levels

Value

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.
6. Link to Strategy

Explores strategy from three perspectives:
7. 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.

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. Photos by Jacob Lund From Noun Project.
8. Recognizes Importance of Culture

- Addresses the growing focus, attention and importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores culture within broader context of overall core
- Depicts culture behavior within a risk spectrum
- Explores possible effects of culture on decision-making
- Explores alignment of culture between individual and entity behavior
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

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
CONSISTENCY AND MEASURED PERFORMANCE

By
Richard J. Anderson | Mark L. Frigo
Risk Assessment Process

Identify Risks
- The possibility that events will occur and affect the achievement of strategy and business objectives

Gather Data and View of Strategic Risks
2

Understand the Strategies of the Organization
1

Prepare Preliminary Strategic Risk Profile
3

Validate and Finalize the Strategic Risk Profile
4

Develop ERM Action Plan
5

Implement ERM Action Plans
7

Communicate the Strategic Risk Profile and Action Plans
6

Identify and Select Risk Responses
- Mitigation Activities
- Risk Monitoring

Ongoing Monitoring and Assessment of Changes
- Constantly changing business environment requires ongoing monitoring
- Need to identify and assess substantial changes
- Revise strategies and risk profile as appropriate

Communicate Risk Information
- Directors
- Executive Management
- Line Management
- Risk and Control Units

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.
- Each organization needs a tailored approach.
- ERM is not a compliance exercise.
- ERM is a mindset
- ERM facilitates information-sharing
- ERM facilitates decision-making
Questions

Please send all questions and requests for further information to the Division of Audit:
auditandcompliance@famu.edu
Division of Audit Contacts

Joseph Maleszewski
VP of Audit
E: joseph.Maleszewski@famu.edu
P: 850-412-7802

Deidre Melton
Director of Audit
E: deidre.melton@famu.edu
P: 850-599-3131
Thank you!