AGA®

Clarifying the Role of Enterprise Risk Management

Introductions/Opening Remarks

Speakers: Doug Webster, Director, Risk Officer, US Agency for International Development

Mike Wetklow, Deputy CFO, National Science Foundation

Learning Objectives

1. Understanding the role of risk management
2. Clarifying the distinction between internal controls, risk management, and Enterprise Risk Management
3. Considerations for a CRO
4. How to get Started

AGA®

Learning Objective 1: Understanding the Role of Risk Management

- The impact of Change
- The goal of stakeholder value

Leading in the Modern World

Which environment most reflects your world in making progress?

The Challenge of Change

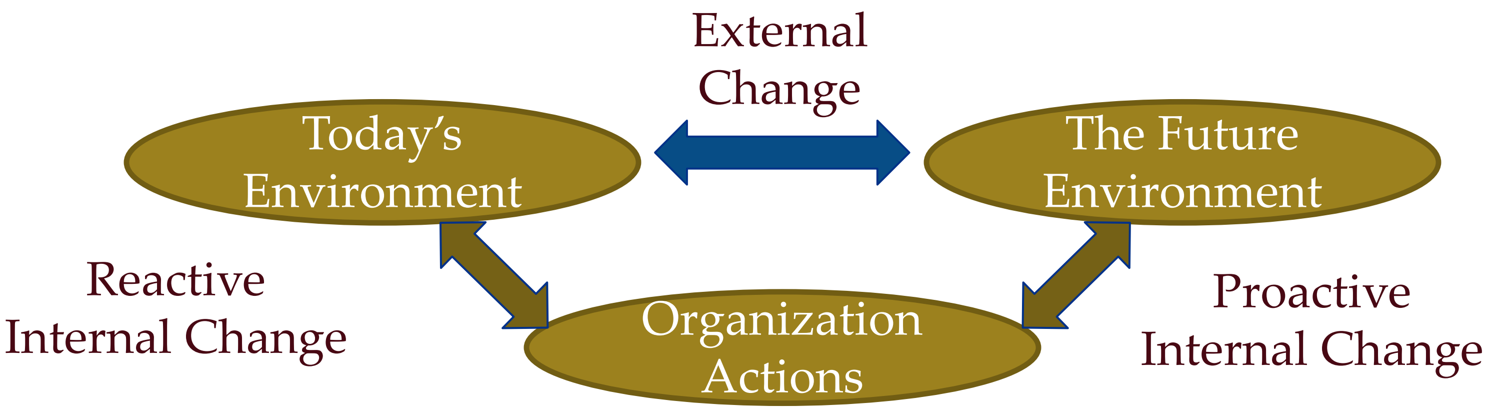
Life would be simple if only it were not for…

Change

External Change

Internal Change

The Challenge of Change



External Change

Today's Environment

The Future Environment

Reactive Internal Change

Organization Actions

Proactive Internal Change

Many organizations act as if in *Groundhog Day*, focused on improving effectiveness and efficiency for today's organization

…but without much attention to tomorrow's needs

A good hockey player plays where the puck is. A great hockey player plays where the puck is going to be.

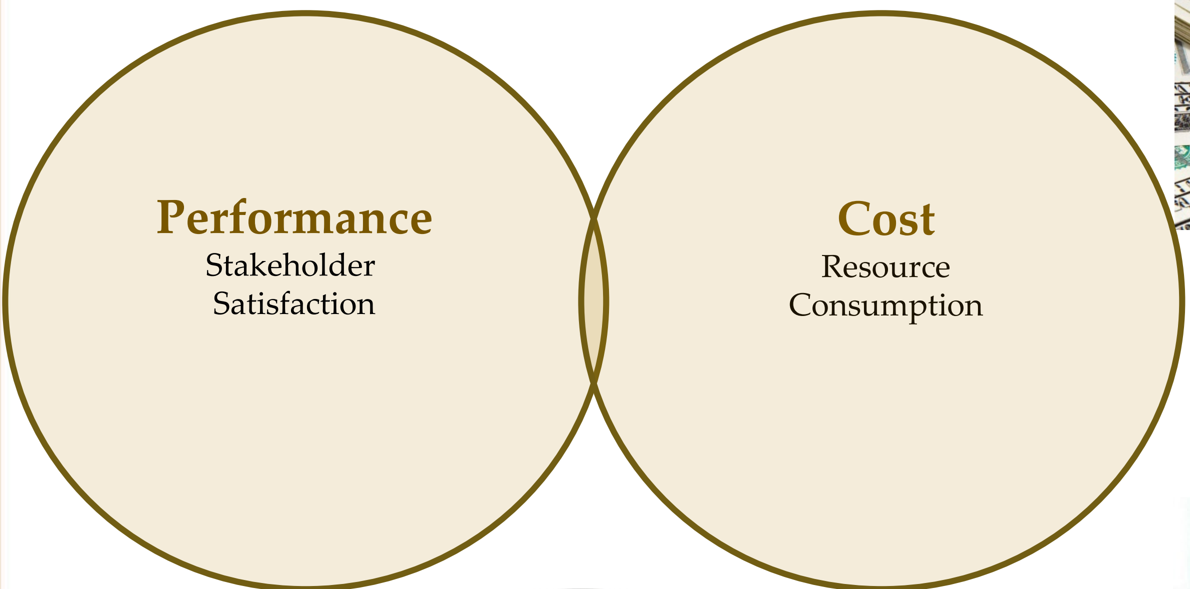
~ Wayne Gretzky

Value Maximization

Performance
Stakeholder
Satisfaction

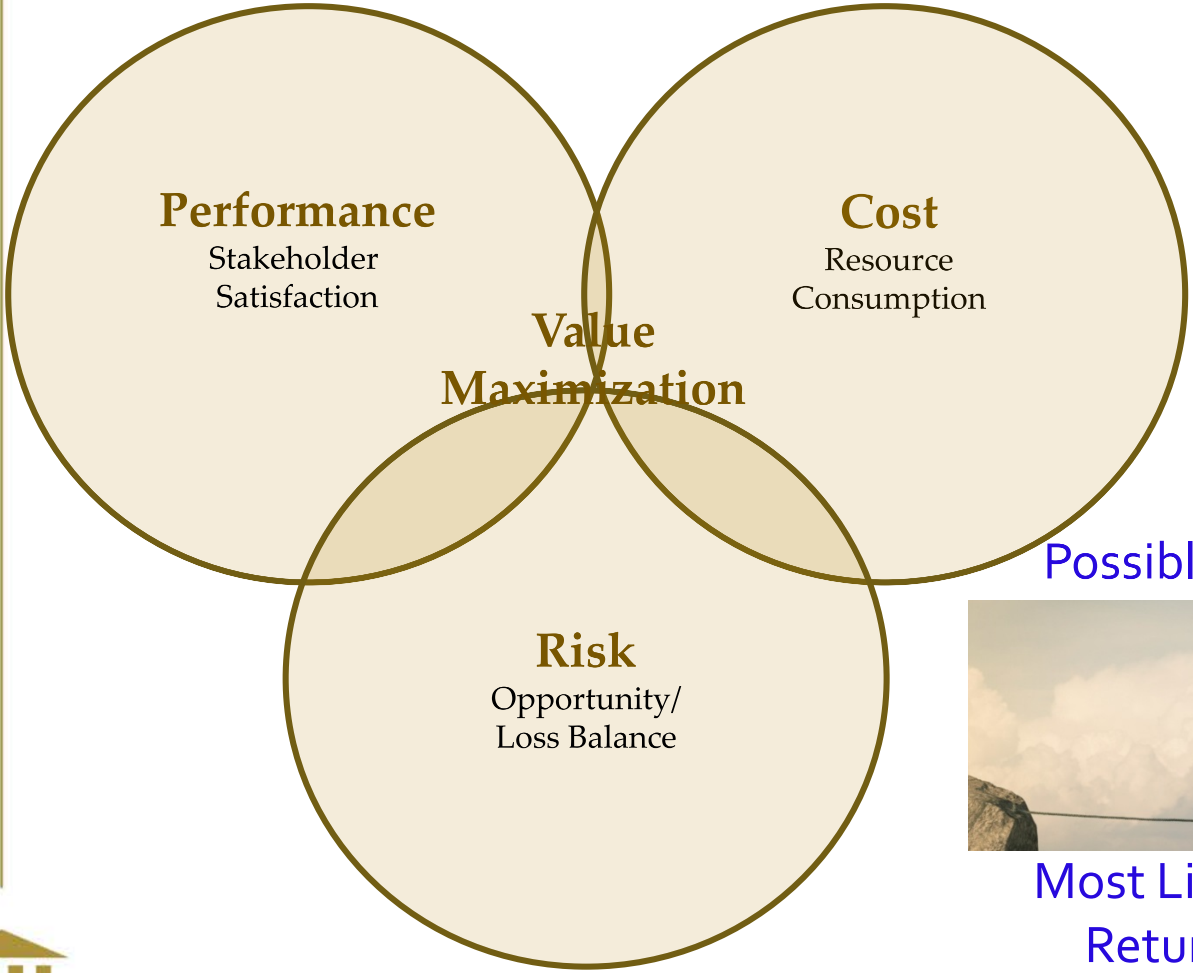
…and others

Value Maximization


Performance
Stakeholder
Satisfaction

Cost
Resource
Consumption

Value Maximization



Performance
Stakeholder Satisfaction

Cost
Resource Consumption

Value Maximization

Risk
Opportunity/ Loss Balance

$$\frac{\text{Performance} \quad - \quad \text{Cost}}{\text{Reward (Return)}}$$

ROI

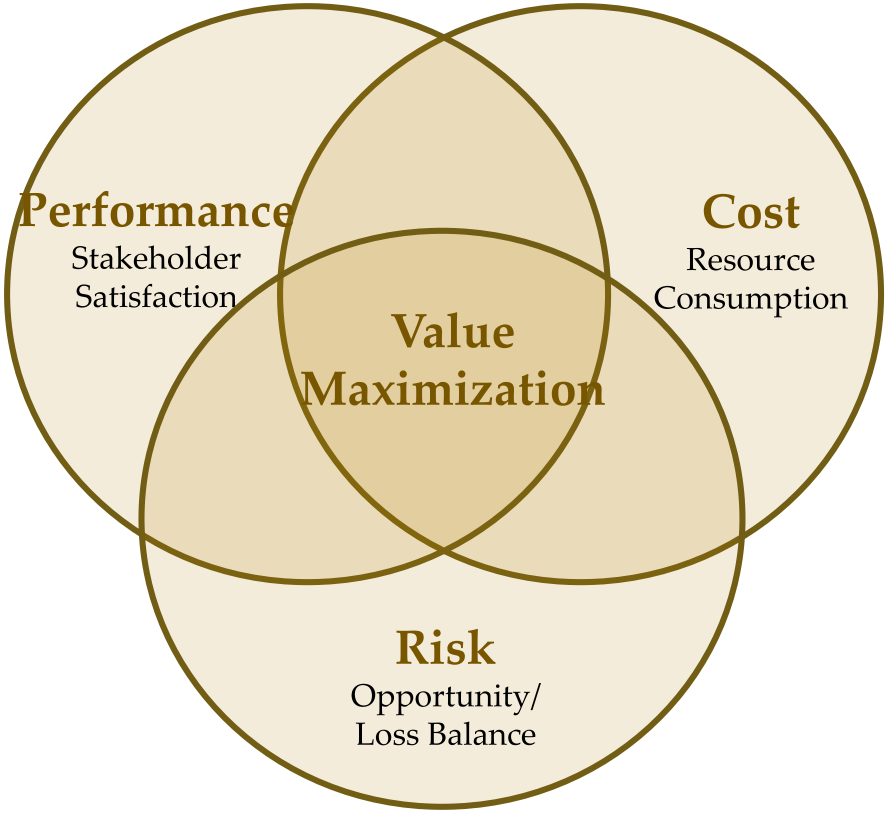
$$\left(\frac{\text{Return}}{\text{Cost}}\right)$$

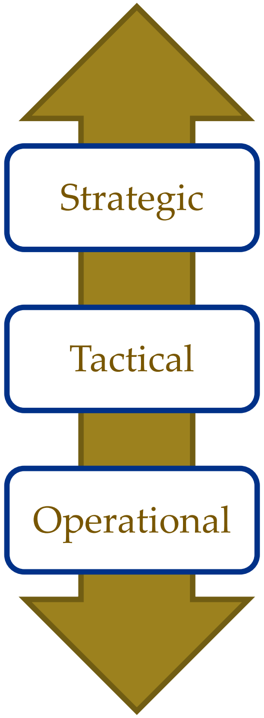
Possible Return

Most Likely Return

Risk

Value Maximization





Learning Objective 2: Clarifying the distinction between internal controls, risk management, and Enterprise Risk Management

- A Risk Management Process
- Internal Controls as an Element of Risk Management
- The Role of Enterprise Risk Management

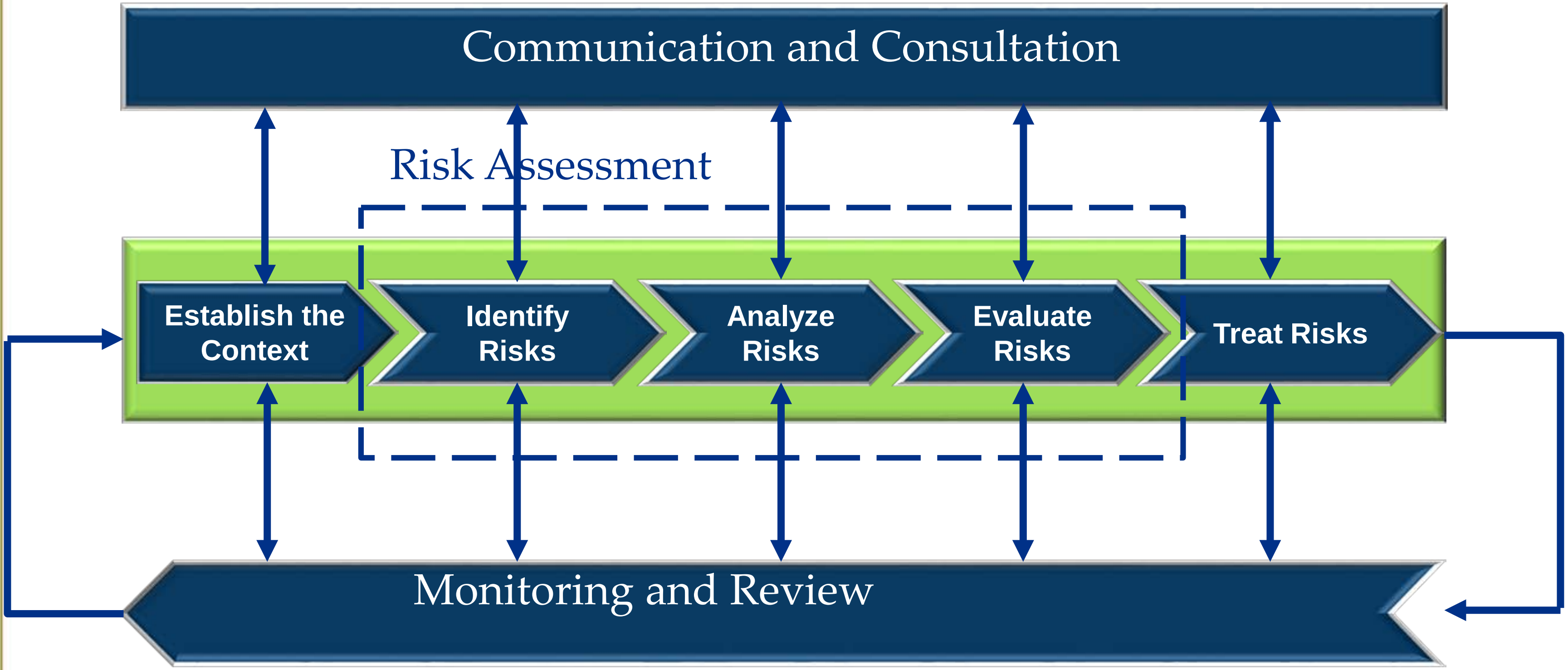
The “What” of ERM

Does a Label Really Matter?

If you gave the command **"SECURE THE BUILDING"**, here is what the different military services might do:

NAVY	Turn out the lights and lock the doors.
ARMY	Surround the building with defensive fortifications, tanks and concertina wire.
MARINE CORPS	Assault the building, using overlapping fields of fire from all appropriate points on the perimeter.
AIR FORCE	Take out a three-year lease with an option to buy the building.

The Risk Management Process



Communication and Consultation

Risk Assessment

Establish the Context

Identify Risks

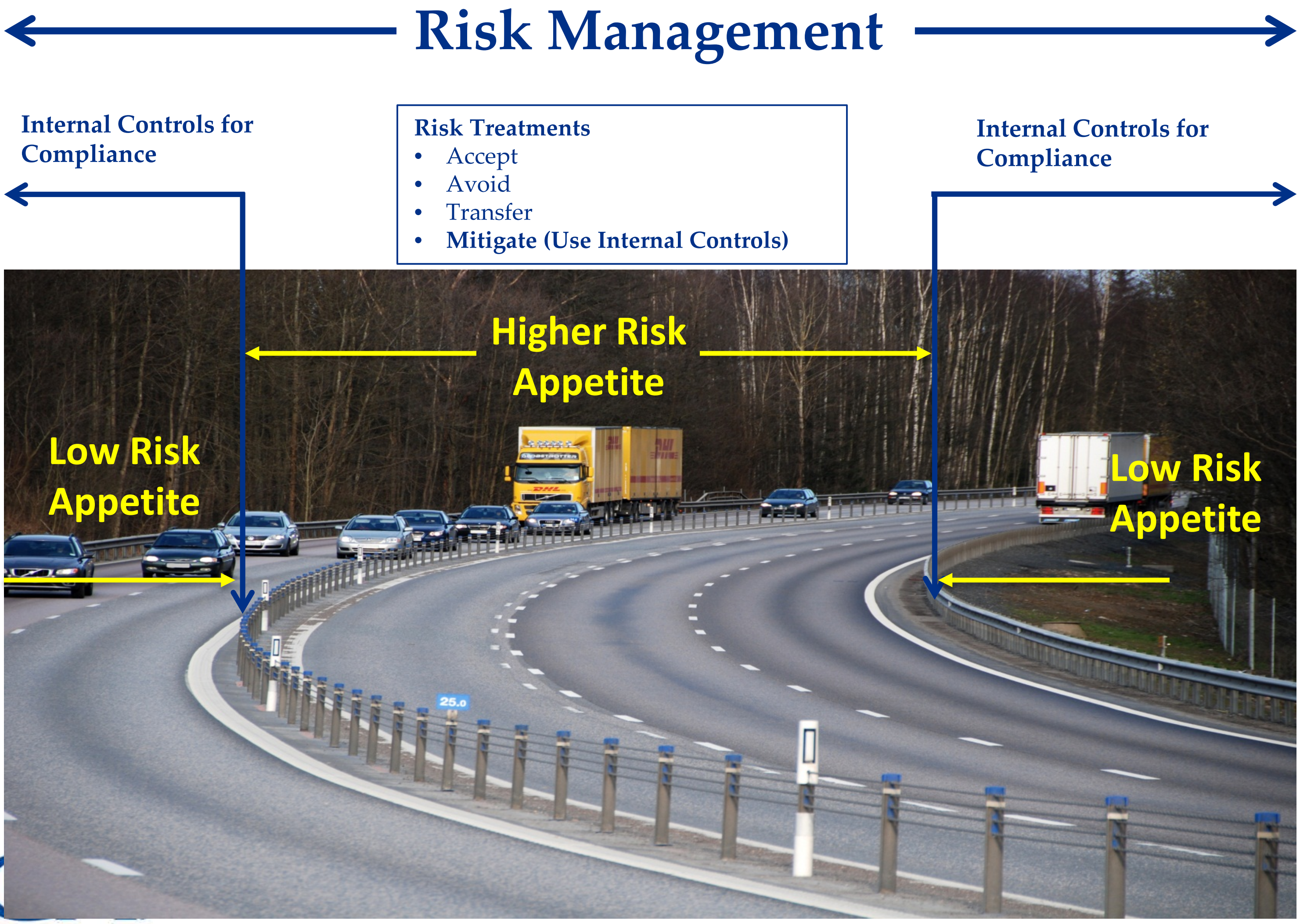
Analyze Risks

Evaluate Risks

Treat Risks

Monitoring and Review

Risk Management vs. Internal Controls



Risk Management

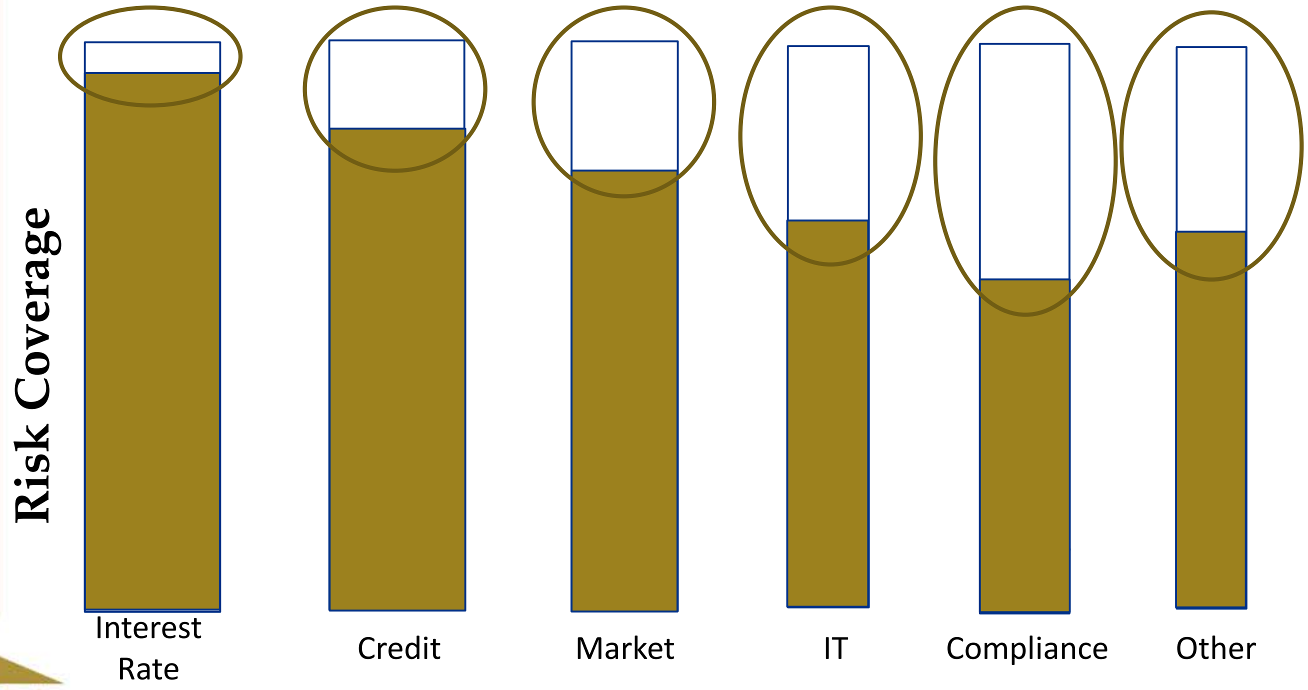
Internal Controls for Compliance

Risk Treatments

- Accept
- Avoid
- Transfer
- **Mitigate (Use Internal Controls)**

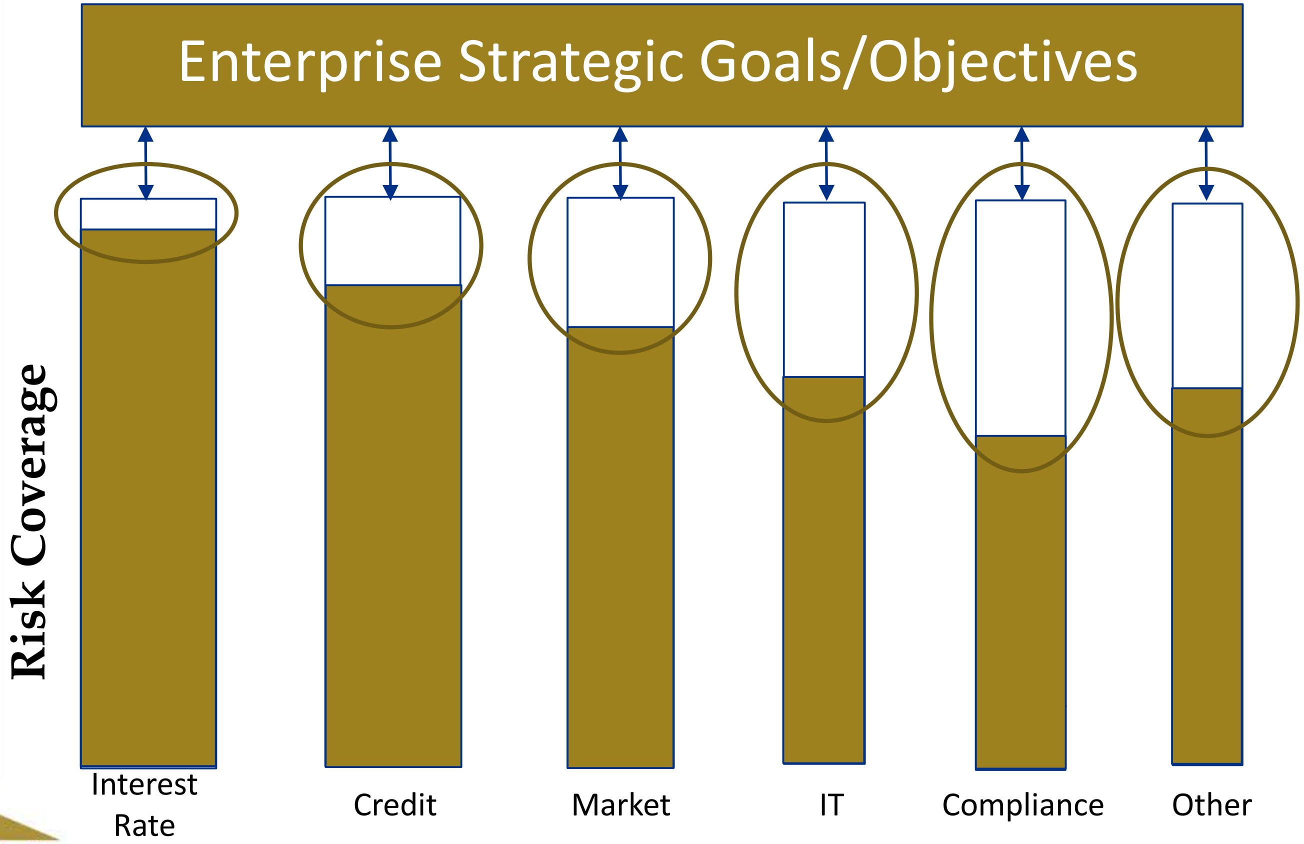
Internal Controls for Compliance

Challenges in Traditional Risk Management



- Differences in general criticality of the risk category to the organization mission and stakeholders
- Differences in maturity in the practice of risk management in each silo (inconsistent policies and practices)
- Differences in risk appetite lead to differences in risk mitigation
- Potential ROI on risk treatments can vary greatly

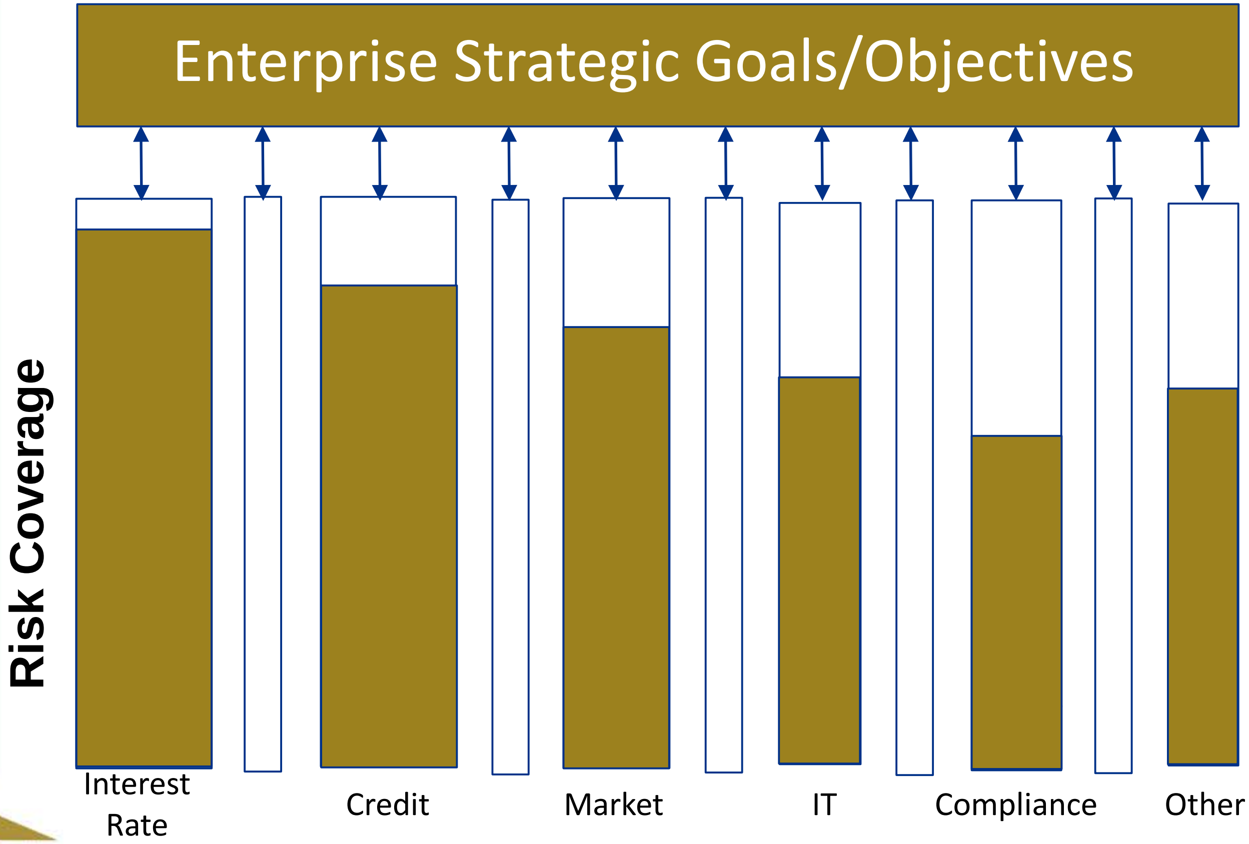
Some Risks Addressed More Completely Than Others



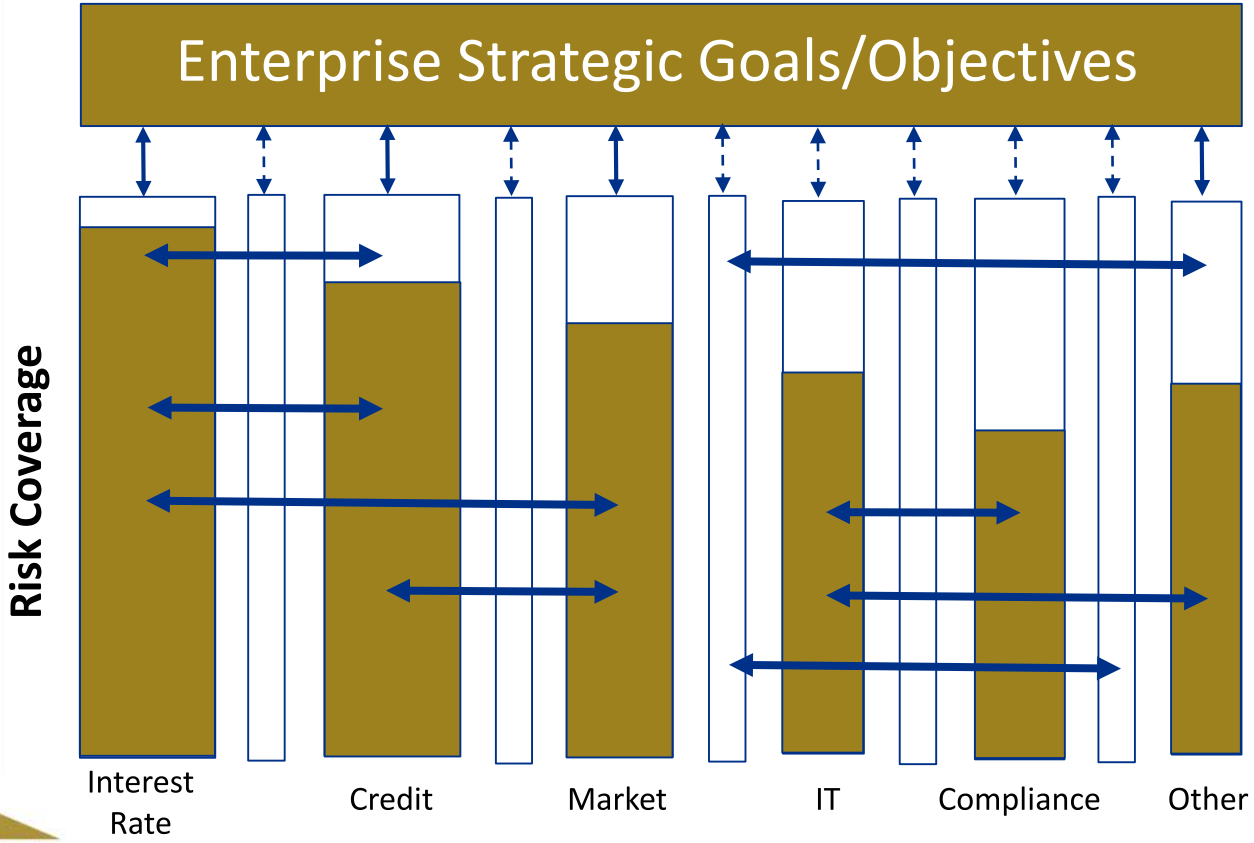
Unmanaged Risk:

- Differences in thoroughness of risk identification
- Differences in risk appetite lead to differences in risk mitigation
- Potential ROI on risk treatments can vary greatly

Top-Down Risk Assessment Identifies Risk in the "White Space"

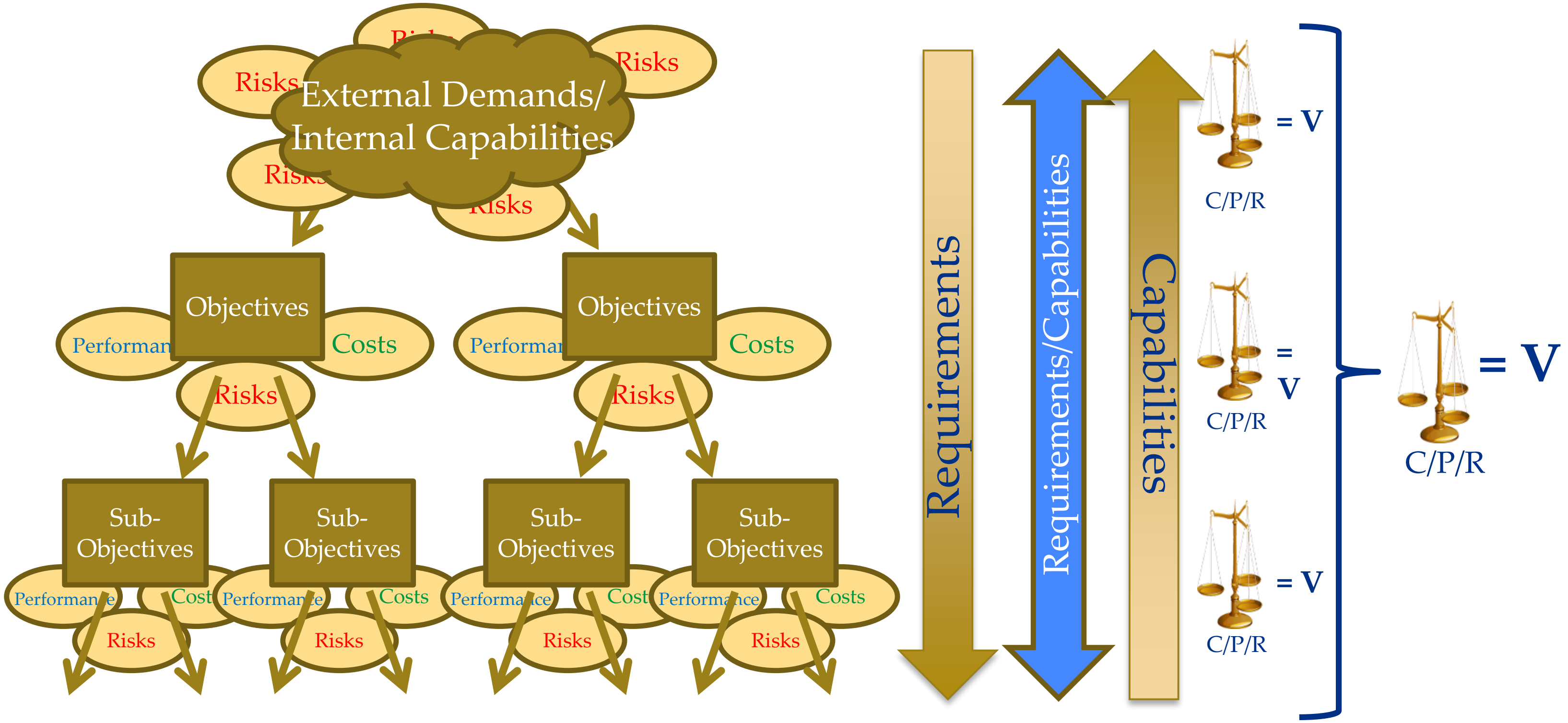


Risks and Risk Mitigations can have Cross-Functional Impacts (+ and -)



Investments in risk management should maximize ROI at the enterprise level

Strategy, Performance, Cost and Risk Must all Interconnect



Removing the Ambiguity Around ERM

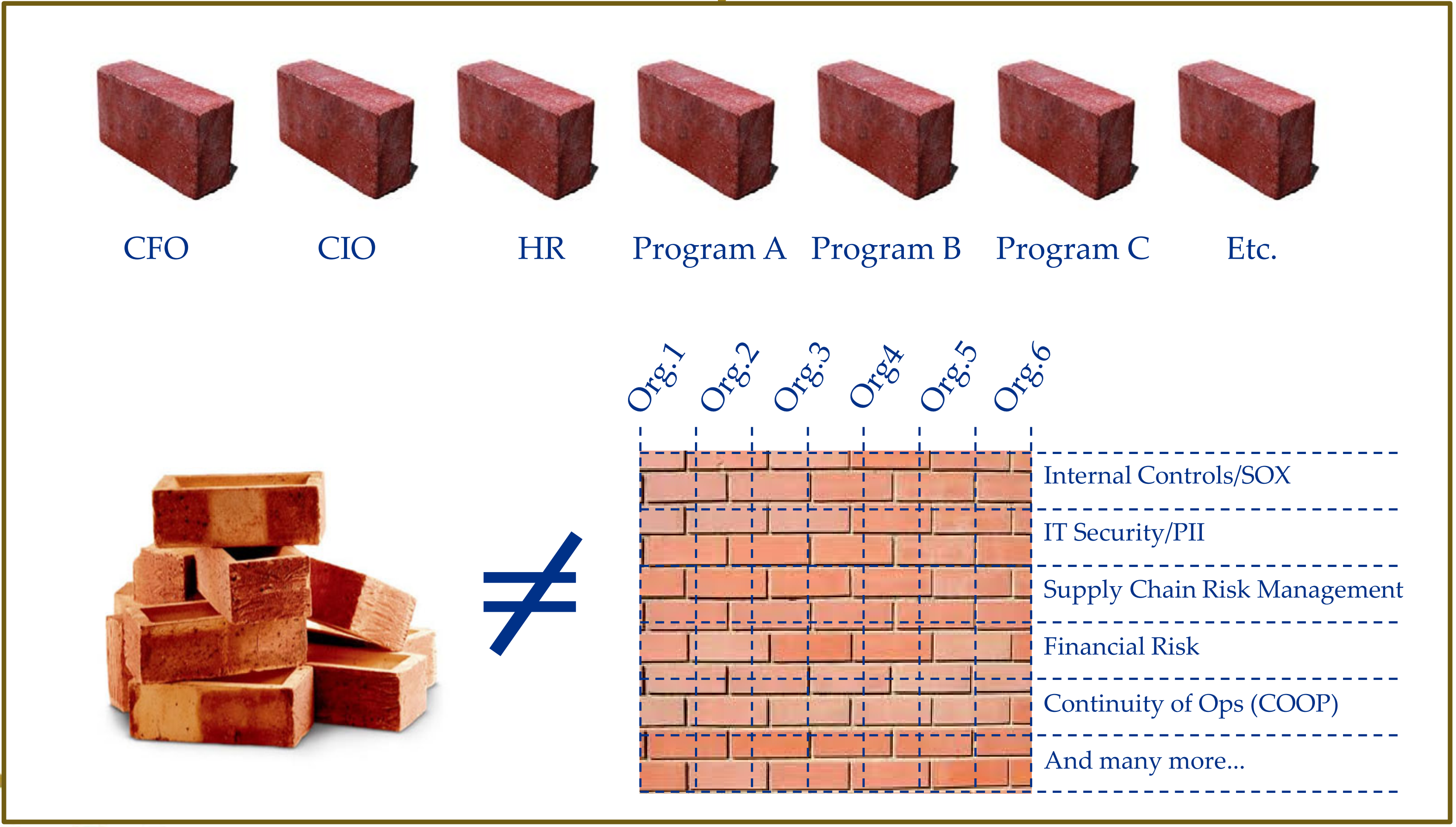
1. ~~Compliance and Internal Controls~~
2. ~~Risks exclusively at the enterprise level (e.g., strategic risks)~~
3. ~~Functional risks that cross the enterprise (e.g., IT risk)~~
4. ~~Integration of some partial set of risks (e.g., financial risks or operational risks)…frequently seen in financial services~~
5. ~~Traditional risk management across all of the enterprise~~

While <u>all</u> of the above are important elements of risk management, they are <u>not synonyms for ERM</u>

6. **"Enterprise Risk Management (ERM) is a discipline that addresses the full spectrum of an organization's risks, including challenges and opportunities, and integrates them into an enterprise-wide, strategically-aligned portfolio view. ERM contributes to improved decision-making and supports the achievement of an organization's mission, goals, and objectives."**

~ Association for Federal Enterprise Risk Management (AFERM)

ERM vs. Risk Management Across the Enterprise



CFO CIO HR Program A Program B Program C Etc.

≠

Org.1 Org.2 Org.3 Org4 Org.5 Org.6

Internal Controls/SOX

IT Security/PII

Supply Chain Risk Management

Financial Risk

Continuity of Ops (COOP)

And many more…

ERM is more than Reporting

- Too often, organizations claim ERM implementation due to reporting key risks to top executives/board
  - Low level risks may be so broadly present across the organization that they would rise to enterprise level risks if aggregated, but that aggregation is never accomplished.
  - Applying ERM only at the highest organizational level limits the opportunity to integrate risks at lower organizational levels. This precludes lower level capabilities being leveraged to deliver maximum value at the highest levels.
- ERM is about enterprise risk management. Risk management is much more than simply reporting to the board or equivalent.

Learning Objective 3: Considerations for a CRO

- The need for centralized coordination
- The potential roles for a CRO and risk organization
- Locating the CRO

Centralized Coordination

1. The essence of ERM is coordination and prioritization across silos
2. Such coordination does not happen alone; a central function is essential for facilitating the cross-functional dialog that must occur for ERM to be effective

The Role of a CRO

1. Establish/facilitate adoption of a common risk framework and process
2. Facilitate cross-functional dialog on risks
3. Monitor consistent application of risk management policy across the enterprise
4. Educate and champion the role of risk management in maximizing organizational stakeholder value
5. Serve as an impartial advisor to top management on risk and risk management
6. Serve as a safeguard for signaling risks inconsistent with the risk appetite

Note: CROs do not own the residual risk. Accountability for risk rests with those making the decisions that incur risk.

Locating the CRO position

- A CRO—to be effective—must have sufficient influence to bring together the various “barons” leading the silos, and facilitate a collaborative approach
  1. Sufficiently senior to engage directly with functional leads
  2. Viewed as a direct representative of the agency’s leader for risk management
  3. Viewed as not favoring any particular part of the organization
- An ideal location would report directly to the agency head or COO

  Note: While some central risk management policy functions report through the CFO, it is essential this function not be viewed as reflecting only a financial or CFO perspective.

Learning Objective 4: How to Get Started

I. **Keys to Success:** Overarching themes to provide management with a strong foundation for an effective ERM program as they develop and tailor their specific approach to implementing ERM.

II. **Initial Action Steps:** Action oriented, “how to” steps to implement an initial ERM effort. These steps support development and implementation of a tailored ERM initiative.

III. **Continuing ERM Implementation:** Next steps to further develop and broaden the organization’s initial ERM effort.

Source: COSO, Thought Leadership in ERM, Embracing Enterprise Risk Management
http://www.coso.org/documents/embracingerm-gettingstartedforwebpostingdec110_000.pdf

How to Get Started: Keys to Success

1. Support from the Top is a Necessity
2. Build ERM Using Incremental Steps
3. Focus Initially on a Small Number of Top Risks
4. Leverage Existing Resources
5. Build on Existing Risk Management Activities
6. Embed ERM into the Business Fabric of the Organization
7. Provide Ongoing ERM Updates and Continuing Education for Leadership and Senior Management

Source: COSO, Thought Leadership in ERM, Embracing Enterprise Risk Management
http://www.coso.org/documents/embracingerm-gettingstartedforwebpostingdec110_000.pdf

How to Get Started: Initial Action Steps

1. Seek Board and Senior Management Leadership, Involvement and Oversight
2. Select a Strong Leader to Drive the ERM Initiative
3. Establish a Management Risk Committee or Working Group
4. Conduct the Initial Enterprise-wide Risk Assessment & Develop an Action Plan
5. Inventory the Existing Risk Management Practices
6. Develop Your Initial Risk Reporting
7. Develop the Next Phase of Action Plans & Ongoing Communications

Source: COSO, Thought Leadership in ERM, Embracing Enterprise Risk Management
http://www.coso.org/documents/embracingerm-gettingstartedforwebpostingdec110_000.pdf

How to Get Started: Continuing ERM Implementation

- A program of continuing ERM education for leaders and executives
- ERM education and training for business-unit management
- Policies and action plans to embed ERM processes into the organization’s functional units
- Continuing communications across the organization on risk and risk management processes and expectations
- Development and communication of a risk management philosophy for the organization
- Identification of targeted benefits to be achieved by the next step of ERM deployment

Source: COSO, Thought Leadership in ERM, Embracing Enterprise Risk Management
http://www.coso.org/documents/embracingerm-gettingstartedforwebpostingdec110_000.pdf

How to Get Started: Continuing ERM Implementation (cont'd)

- Development of board and corporate policies and practices for ERM
- Further discussion and articulation of a risk appetite for the organization and /or significant business units, including quantification
- Establishment of clear linkage between strategic planning and risk management
- Integration of risk management processes into an organization's annual planning and budgeting processes
- Expansion of the risk assessment process to include assessments of both inherent and residual levels of risk
- Exploration of the need for a dedicated Chief Risk Officer or ERM functional unit

Source: COSO, Thought Leadership in ERM, Embracing Enterprise Risk Management
http://www.coso.org/documents/embracingerm-gettingstartedforwebpostingdec110_000.pdf