ESTABLISHING ENTERPRISE RISK MANAGEMENT IN MANAGEMENT PRACTICES

Mark Reger
U.S. Deputy Controller
Office of Management and Budget
November 3, 2015

"I have emphasized the importance of having appropriate risk management processes and systems to identify challenges early, bring them to the attention of Agency leadership, and develop solutions," President Obama.

Background

- The Federal Managers Financial Integrity Act of 1982 (FMFIA) requires the Government Accountability Office (GAO) to establish internal control standards and OMB to provide implementation guidance (we do this in Circular A-123).

- Between 1982 and 2004 OMB A-123 promoted “management controls” across all management practices (e.g, financial, procurement, information technology, human capital, and operations).

- In 2004, OMB A-123 focused narrowly on financial management to avoid internal control audit legislation.

- Since 2004 OMB A-123 has become to be known as the “CFO’s Circular” and often referred to as a “compliance drill.”

- In 2004, in the private sector, Enterprise Risk Management began evolving from internal controls practices to avoid surprises in corporate scandals (e.g., Enron).

- More recently, many agencies are beginning to establish Chief Risk Officers (CROs) or risk committees, which is a good practice, however CROs are often focused on a an individual silo, e.g., credit risk or within a Component of a Department.

Background:
Agency and Industry Input

- GAO Green Book Advisory Council (7/2013 to 9/2014)
- Three Agency Workgroups (11/2013 to 3/2014)
- CFO Council AFERM Forum (April 2014)
- CFO Council ERM Project (2/2014 to 2/2015)
- AGA Forum on Internal Control (9/2014)
- President's Management Council Briefing (5/2015)
- Provided A-123 to Agencies for Comment (6/2015)
- Partnership for Public Service ERM Forums (6/2015 and 9/15)

AFERM
Association for Federal Enterprise Risk Management

PARTNERSHIP FOR PUBLIC SERVICE

What People Are Saying

Theme 1: ERM is a growing priority in the Government.

- 80% of respondents not practicing ERM, plan to develop ERM capability in the future.

Theme 2: ERM enables Federal Agencies to better define and proactively respond to risks.

- 76% of respondents who practice ERM realized benefits in
  - reduced duplicity in risk and compliance activities,
  - enhanced decision making by using data and information produced by the ERM program,
  - strategic oversight that does not exist today, raising concerns early, improved roles and responsibilities.

Theme 3: Agencies with ERM programs built dedicated programs and processes to effectively manage risks.

- 83% of respondents with ERM programs have dedicated central resources of that amount (41%) have a centralized leadership structure and 42% have central leadership structure with supplemented by decentralized support. Only 36% or organizations surveyed have a "Chief Risk Officer."

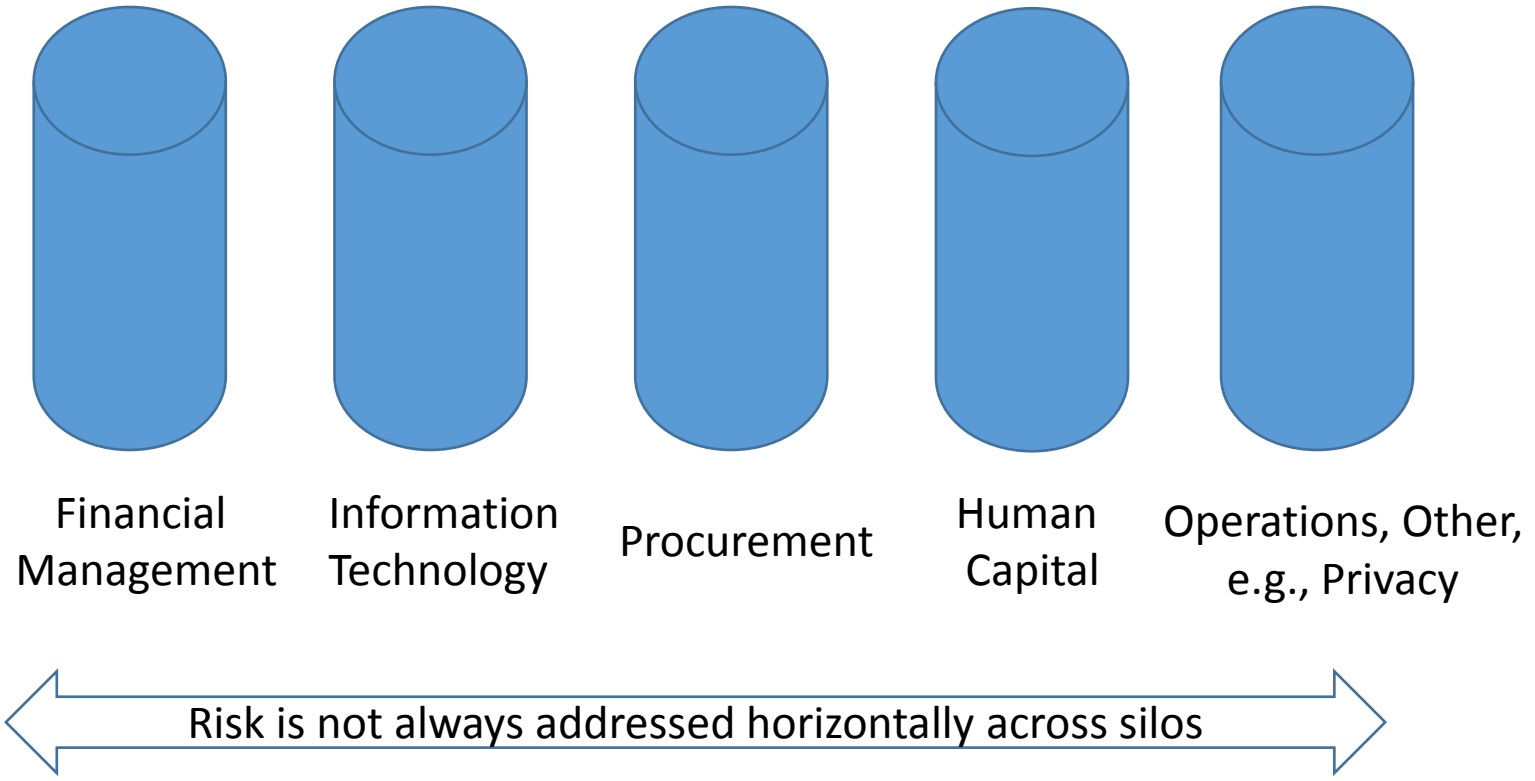
Theme 4: Barriers continue to inhibit ERM.

- 57% of respondents indicate siloed: data, decision making, and risk management.
- 23% of respondents indicate a lack of executive level support.
- 50% of respondents agree there is a need for an OMB Circular to influence leadership to adopt ERM.
- 14% of respondents indicate the lack of a business case as a barrier.

Source: Association of Federal Enterprise Risk Management 2015 Survey of Federal Agencies

How Enterprise Risk Management Can Help

Risk is typically addressed within vertical functional, programmatic, or organizational silos.



Moving From Compliance to Managing Risks

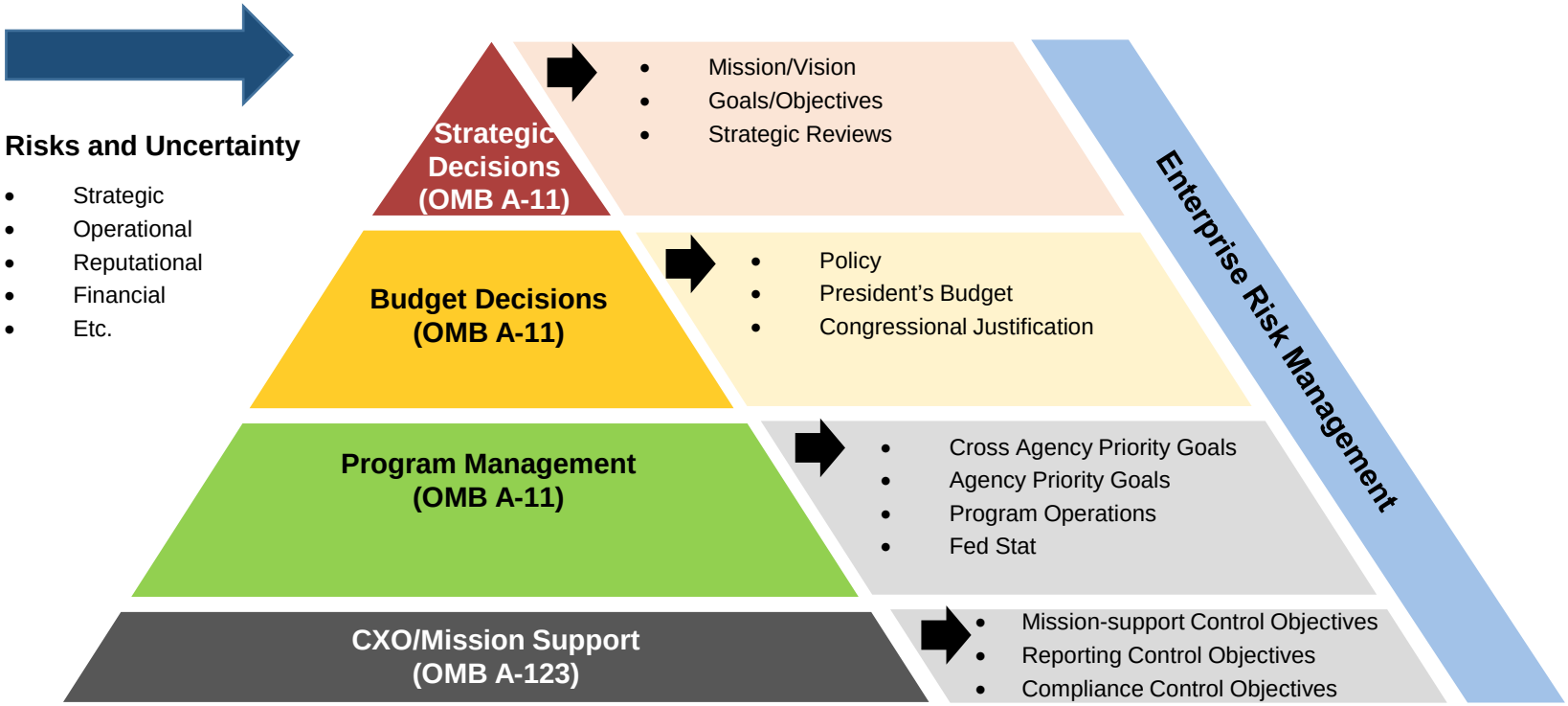
Check the Box (A-123 Today)

- Compliance with New GAO Internal Control Standards
- Treating Risk as only Negative
- Heavy Emphasis on Financial Reporting
- Regarding Risk Management as Separate
- Check the Box on 3 Year A-123 Assessments

Proactively Managing Risks (A-123 Tomorrow)

- Risk Based Approach with New Internal Control Standards
- Defining risk as both positive (e.g., taking on risk to improve government services) and negative
- Balanced Emphasis on Financial Reporting and other mission support areas
- Integrating Risk Management and Internal Control
- Manage Risks Across Silos

Next Steps: Building In ERM Rather Than Adding On



Based on the UK Orange Book

Internal Control Over ~~Financial~~ Reporting

A-123 Considerations: Risk Profiles

Risk Assessments should be documented in a way which records the stages of the process. Documenting risk assessments creates a risk profile for the organization, which:

- Encourages open and candid conversations about risks facing an organization at all levels;
- Facilitates identification of risk priorities (in particular to identify the most significant risk issues with which senior management should know);
- Captures the reasons for decisions made about what is and is not tolerable exposure;
- Facilitates recording of the way in which it is decided to address risk;
- Allows all those concerned with risk management to see the overall risk profile and how their areas of particular responsibility fit into it; and
- Facilitates review and monitoring of risks.

A-123 Considerations: Reviewing and Reporting Risks

The risk management review processes should:

- Ensure that all aspects of the risk management process are reviewed at least once a year;
- Ensure that risks themselves are subjected to review with appropriate frequency; and
- Make provision for alerting the appropriate level of management to new or emerging risks as well as changes in already identified risks so that the change can be appropriately addressed.

Risk Management processes should be put in place to review and deliver assurance on the effectiveness of control and management oversight.

Next Steps:
Enterprise Risk Management Playbook

I. Introduction
II. Enterprise Risk Management Framework
III. Enterprise Risk Management Governance Structure
IV. Managing Risks On A Portfolio Basis Across An Agency
V. Best Practices
VI. Tools and Templates

Next Steps: ERM Training

- What is Enterprise Risk Management?
- What is a CRO and what are the roles and responsibilities of the CFO and other CXOs (i.e., good governance)?
- What does success look like?
- What are the best practices?
- How do I get started?
- How to build ERM into existing processes rather than add on?

- Overview of ERM Standards.
- Comparisons between COSO and ISSO (not vs.).
- The link between ERM and Internal Control Standards.
- What are the tools and templates of ERM?
- Do I have to do it all at once, what's a sample maturity model?

- Strategic Foresight.
- What role do inspector generals play in ERM?
- What are the road rules for management engagement of inspector generals in ERM?

Thank You!

OMB Contact Information:

Mike Wetklow
mwetklow@omb.eop.gov