Establishing Enterprise Risk Management in Management Practices

Introductions/Opening Remarks

Speakers: Cynthia Vitters, Chief Risk Officer, Federal Student Aid

Mike Wetklow, Branch Chief, Office of Management and Budget

Moderator: John Homan, 2015–2016 AGA National President

ERM Task Force Goals

I.   Develop an AGA sponsored ERM Webinar Series to provide training and implementation guidance

II. Conduct an AGA sponsored research survey of the current state of Enterprise Risk Management in the Government

III. Facilitate Faculty Networking Opportunities between the AGA and other associations and business lines.

AGA.

ERM Task Force Members

- Sheila Conley, Deputy CFO, Department of Health and Human Services
- Doug Glenn, Deputy CFO, Department of Interior
- Dan Kaneshiro, Policy Analyst, Office of Management and Budget
- Christine Jones, Associate Deputy Assistant Secretary for Finance, Department of Health and Human Services
- Tim Soltis, Deputy CFO, Department of Education
- Teresa Taber, Deputy Director Office of Financial Management, Department of Interior
- Dr. Doug Webster, Director, Government to Government Risk Management at US Agency for International Development
- Mike Wetklow, Branch Chief, Office of Management and Budget (Chair)

AGA

Learning Objectives

1. What is Enterprise Risk Management?

2. What does success look like?

3. What are the best practices?

4. How do I get started?

5. How to build ERM into existing processes rather than add on?

AGA

Learning Objective 1: What is Enterprise Risk Management?

Risk is the effect of uncertainty on objectives. Risk management is coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives. Enterprise risk management (ERM) is an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that, provides better insight about how to most effectively prioritize and manage risks to mission delivery. While agencies cannot mitigate all risks related to achieving strategic objectives and performance goals, they should identify, measure, and assess challenges related to mission delivery, to the extent possible.

Source: OMB Circular No. A11, Section 270.24

Illustrative ERM Model

Based on UK Orange Book

What is Enterprise Risk Management at FSA?

Agencies can define Enterprise Risk Management in different ways.

Federal Student Aid define Enterprise Risk Management as a coordinated, culture-based approach to holistically addressing all of an organization's risks – including: operational, financial, strategic, compliance, and reputational risks.

What Do We Mean By Enterprise Risk Management - FSA?

A successful ERM program can assist an organization to:

- work toward a more integrated and comprehensive assessment of risks, and an objective, consistent approach to managing them;

- through a consistent risk governance framework, help establish enhanced clarity around risk management roles and responsibilities;

- help create a more common language and improved customized view of risk across the agency;

- monitor more completely an organization's risk level as compared to its risk appetite, to include correlations and dependencies across products and risk types; and

- increase focus on both traditional and emerging risk types.

AGA.

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.

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

AGA.

What People Are Saying

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

AGA.

Learning Objective 2: What Does Success Look Like?

- A "Portfolio" Approach to Managing Risks
- A Holistic View of Integrated Risks/Interdependencies
- Higher Level of Value Added
  - Better, More-informed Decisions
  - Greater Management Consensus
  - Increased Management Accountability
- Better Understanding of Business Risks
- Strategic Risks Aligned with Strategic Goals and Objectives

Learning Objective 3: Best Practices/Lessons Learned in Implementation

I. Educate the Organization
II. Illustrate Credibility
III. Built Trust / Gained Buy- In
IV. Demonstrate Value
V. Identified Quick Wins

AGA®

I. Educate the Organization

- Define Goal and Purpose
- Develop a Common Risk Understanding (definitions and terminology)
- Meet with Key Leaders Across the Organization to Share Goal, Purpose, and Risk Management Concepts to Socialize
- Provide Risk Management Training to Business Unit Senior Leaders and their Respective Staff

II. Illustrate Credibility

- Develop a Project Plan and Timeline for Implementation (Phased Approach)
- Develop Sound Risk Tools to be Used for Implementation
- Hire Best Resources Available
- Meet with Senior Leaders Across Organization to Socialize Information

AGA.

III. Build Trust / Gain Buy In

- Hold Honest Dialogue on Issues
- Demonstrate No Surprises
- Provide examples of What's In It For Them / How the Program would Add Value

AGA.

IV. Demonstrate Value

- Build on Ongoing Risk Efforts Underway
- Develop Sound Risk Tools to be Used for Implementation
- Identify Quick Wins - Perform High-Level Risk Assessment Identifying Top Risks
- Meet with Senior Leaders Across Organization to Share Information / Progress

V. Identify Quick Wins

- Perform High-Level Risk Assessment Identifying Top Risks
- Conduct Targeted Risk Assessments for Selected Business Units

AGA.

Additional Considerations

- Consider establishing a Risk Office or ERM organization
- Head of Risk Organization should be a member of Executive Management
- Establish an ERM Committee to provide sponsorship, approval, and oversight
- Ensure the ERM Plan/Strategy/Framework are well-defined and communicated

Learning Objective 4: How Do I Get Started?

- Executive Level support is essential
- Dedicated Internal Resources are required (e.g., Risk Office, Internal Audit, etc.)
- Consider Using External Expertise
- Develop a High-Level ERM Implementation Strategy
- Start with a High-Level Risk Assessment

AGA®

How Do I Get Started?

- Establish a process/framework for implementing ERM
- Adopt a common risk language that includes:
  - ERM Definitions and Risk Terminology
  - Established Risk Categories
- Develop a Communications Plan
- Provide ERM Training and Tools

How Do I Get Started?

Considerations:

- ERM is not a short term project
- It's okay to start slowly – just get started!
- Implementing ERM is a cultural change
- Expect resistance
- Don't oversell ERM benefits

AGA

ERM Tools: Risk Profiles

Risk Profiles: The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives and arising from its activities and operations. A risk profile is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process, with significance determined based on the likely impact of the identified risk on meeting the strategic and operational objectives of the agency.

- encourages open and candid conversations about risks facing an organization at all levels;
- facilitates the ranking of risk priorities (in particular to identify and escalate the most significant risk issues about which senior management should know);
- captures the reasons for decisions made about risk tolerances;
- facilitates recording of the way in which it is decided to address risk;
- allows leadership at all levels to understand the overall risk profile and how their areas of particular responsibility fit into it; and
- facilitates the review and   regular monitoring of risks.

AGA®

Illustrative Risk Profile

REPORTING OBJECTIVE – Provide relivable external financial reporting

RISK	Inherent assessment		RISK MITIGATION	Residual assessment		PROPOSED ACTION	OWNER	Proposed Action
	Impact	Likelihood		Impact	Likelihood			Category
Agency X identified material weaknesses in internal control.	High	High	REDUCTION: Agency X has developed corrective actions to provide program partners technical assistance.	High	Medium	Agency X will monitor corrective actions to maintain audit opinion.	Primary –Chief Financial Officer	Primary –Internal Control Assessment

COMPLIANCE OBJECTIVE – Comply with the Improper Payments legislation

| RISK	Impact	Likelihood	RISK MITIGATION	Impact	Likelihood	PROPOSED ACTION	OWNER	Category
Program X is highly susceptible to significant improper payments.	High	High	REDUCTION: Agency X has developed corrective actions to ensure improper payment rates are monitored and reduced.	High	Medium	Agency X will develop budget proposals to strengthen program integrity.	Primary – Program Office	Primary – Internal Control Assessment and Strategic Assessment

AGA

ERM Tools: Risk Profiles

STRATEGIC OBJECTIVE – Improve program outcomes

RISK	Inherent assessment		RISK MITIGATION	Residual assessment		PROPOSED ACTION	OWNER	Proposed Action
	Impact	Likelihood		Impact	Likelihood			Category
Agency X is exceeding program output targets due to positive economic trends.	High	High	Not Applicable (NA)	NA	NA	Agency X will formulate plans to seize opportunity.	Primary – Program Office	Primary – Strategic Assessment

OPERATIONS OBJECTIVE – Manage this risk of fraud in Federal operations

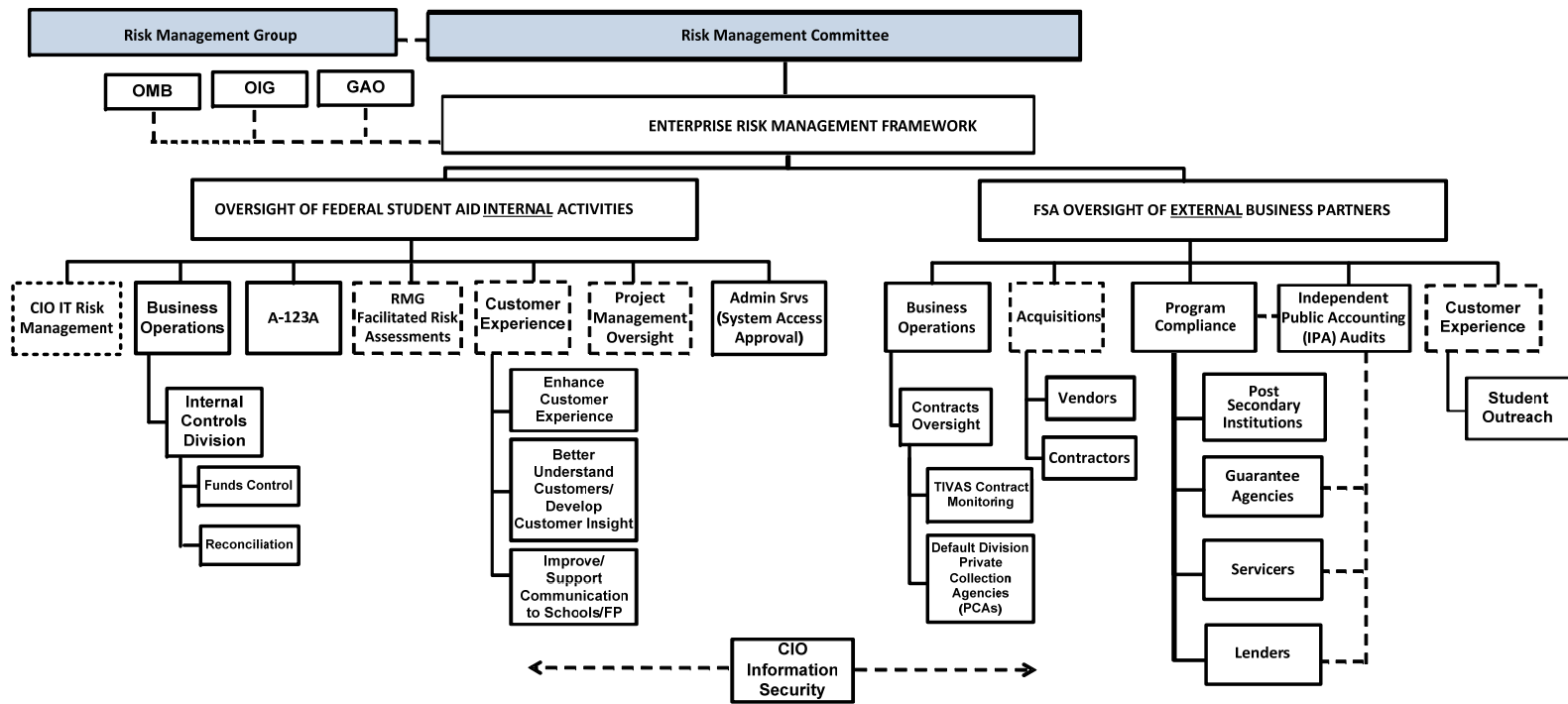| Contract and Bidding fraud. | High | Medium | REDUCTION: Agency X has developed procedures to ensure contract performance is monitored and that proper checks and balances are in place. | High | Medium | Agency X will provide training on fraud awareness, identification, prevention, and reporting. | Primary – Contracting Officer | Primary – Internal Control Assessment |

Learning Objective 5: How to build ERM into existing processes rather than add on?
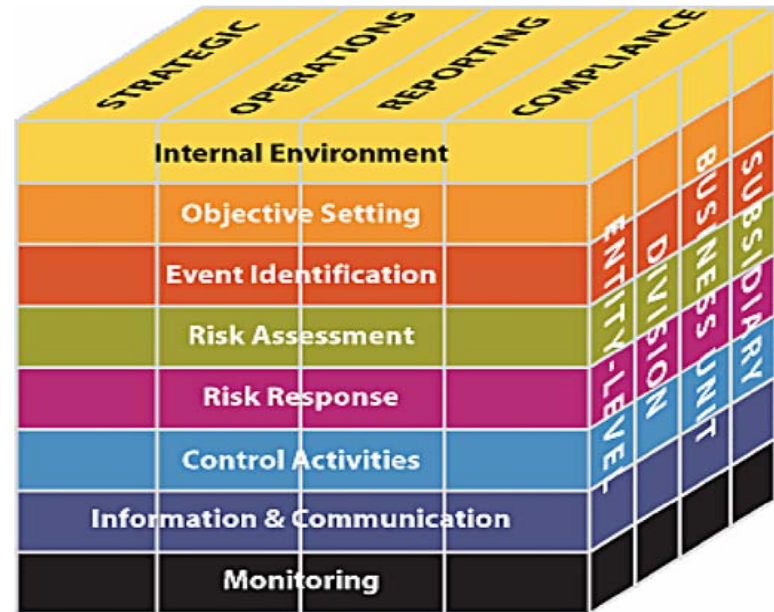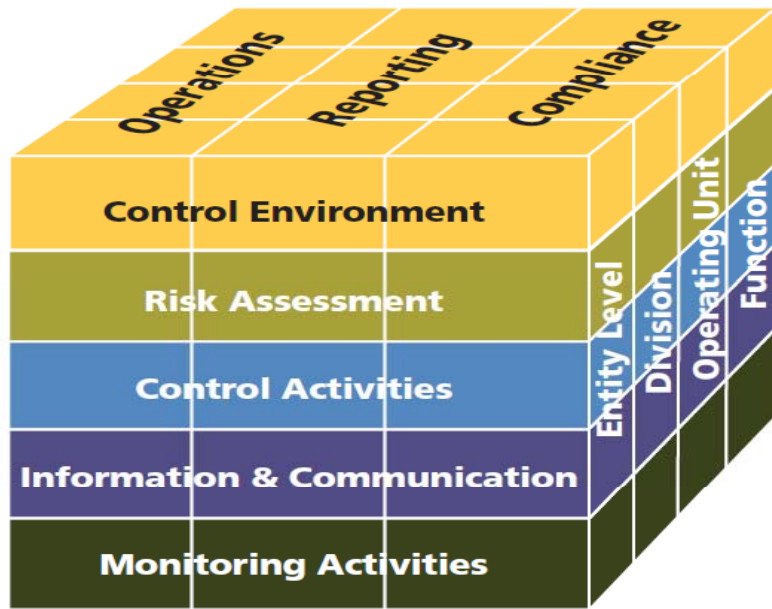
Risk Assessment / Oversight Alignments at FSA

Executive Overview
RM Group Alignment with Business Unit Monitoring & Oversight Activities
"ONE SIZE DOES NOT FIT ALL"

Risk Management Group	Risk Management Committee

- OMB
- OIG
- GAO

ENTERPRISE RISK MANAGEMENT FRAMEWORK

OVERSIGHT OF FEDERAL STUDENT AID INTERNAL ACTIVITIES

- CIO IT Risk Management
- Business Operations
  - Internal Controls Division
    - Funds Control
    - Reconciliation
- A-123A
- RMG Facilitated Risk Assessments
- Customer Experience
  - Enhance Customer Experience
  - Better Understand Customers/ Develop Customer Insight
  - Improve/ Support Communication to Schools/FP
- Project Management Oversight
- Admin Srvs (System Access Approval)

FSA OVERSIGHT OF EXTERNAL BUSINESS PARTNERS

- Business Operations
  - Contracts Oversight
    - TIVAS Contract Monitoring
    - Default Division Private Collection Agencies (PCAs)
- Acquisitions
  - Vendors
  - Contractors
- Program Compliance
  - Post Secondary Institutions
  - Guarantee Agencies
  - Servicers
  - Lenders
- Independent Public Accounting (IPA) Audits
- Customer Experience
  - Student Outreach

CIO Information Security

Draft for RM Discussion Purposes Only

Note: Boxes with dotted lines are not fully matured groups – under development.

AGA®

Wrap Up

1. What is Enterprise Risk Management?

2. What does success look like?

3. What are the best practices?

4. How do I get started?

5. How to build ERM into existing processes rather than add on?