GAO

Presentation for 14th Quarterly Federal Foresight Community of Interest
January 27, 2017

Enterprise Risk Management:

Selected Agencies' Experiences Illustrate Good Practices in Managing Risk

GAO-17-63

What is risk?

- Risk is the effect of uncertainty on objectives with the potential for either a negative outcome or a positive outcome or opportunity.

What is Enterprise Risk Management?

- ERM is part of overall organizational governance and accountability functions and leadership decision-making tool:
  - encompasses all areas where an organization is exposed to risk (financial, operational, reporting, compliance, governance, strategic, reputation, etc.),
  - helps management to understand an organization's portfolio of top-risk exposures that could affect achieving agency goals,
  - recognizes how risks interact (i.e., how one risk can magnify or offset another risk), and also examines the interaction of risk treatments (actions taken to address a risk), such as acceptance or avoidance.

GAO

Background

- Office of Management and Budget (OMB), *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123, (July 15, 2016).
- OMB also updated OMB, Circular No. A-11, *Preparation, Submission, and Execution of the Budget* pt 6,§§ 270 (July 2016).
- These updated requirements help modernize existing management efforts by requiring agencies to implement an ERM capability coordinated with the strategic planning and strategic review process established by the GPRA Modernization Act of 2010, and with the internal control processes required by the FMFIA and in GAO's *Standards for Internal Control in the Federal Government,* GAO-14-704G.

Why ERM?

- The Office of Federal Student Aid (FSA) in the Department of Education adopted ERM in 2004, to help address long-standing risks including poor financial management and internal controls, which led us to place it on our High-Risk List between 1990 and 2005.
- The Internal Revenue Service (IRS) adopted an ERM program in 2013 to address issues related to the review of tax-exempt applications cited in a Department of the Treasury Inspector General for Tax Administration report that would improve IRS operations broadly, as well as provide a common framework for capturing, reporting, and addressing risk areas.
- The Office of Public and Indian Housing (PIH) at the Department of Housing and Urban Development (HUD) finalized its ERM framework and implementation in 2014 in response to several high profile financial and compliance issues with public housing authorities in 2005, as well as concerns over the completeness of its Federal Managers' Financial Integrity Act certifications including internal controls and risk management practices.

Report Objectives, Scope, Methodology

Objectives:

- Update GAO risk management framework to more fully include evolving requirements and essential elements for federal ERM
- Identify good practices that selected federal agencies were taking to illustrate those essential elements

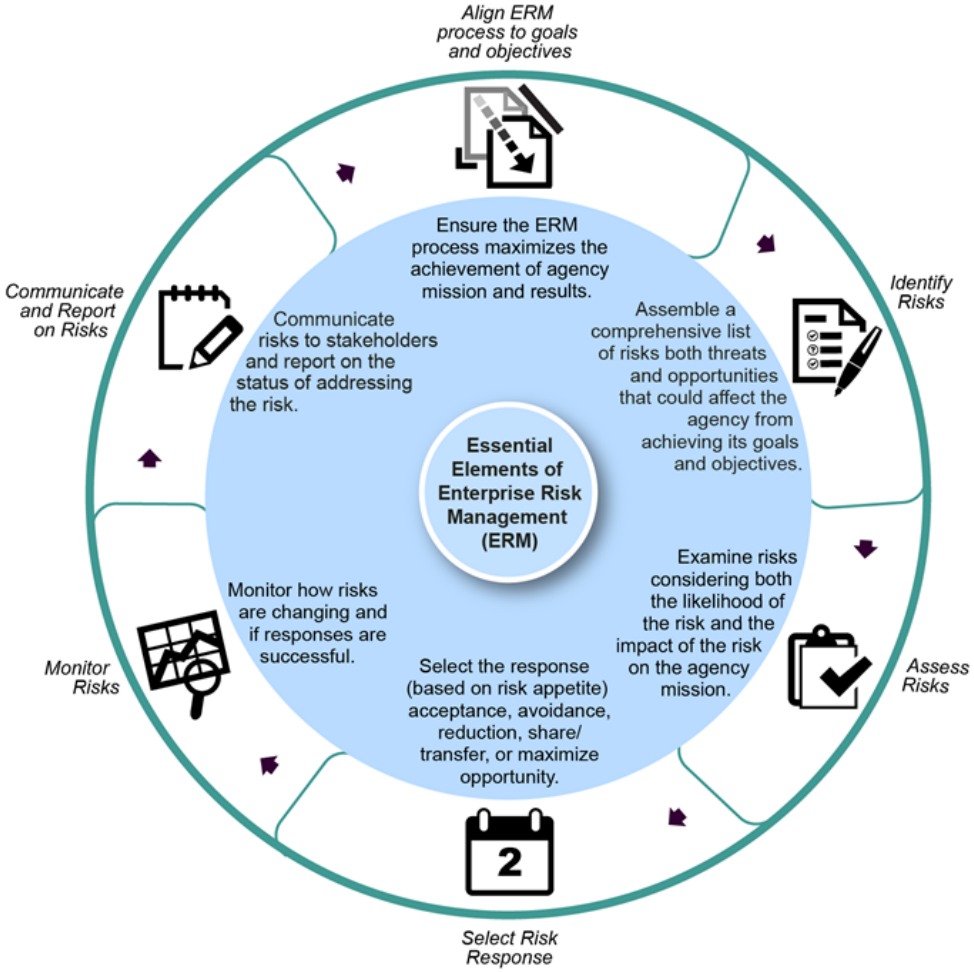
Scope:

- Interviewed 24 Chief Financial Officer agencies to identify agencies engaged in ERM and select illustrations of good practices

Methodology:

- Review of commonly used ERM frameworks, ISO 31000, COSO 2004, UK Orange Book
- Literature review to identify good practices
- ERM subject matter specialists validated essential elements and good practices
- Agency document review and interviews

Essential Elements of ERM



Source: GAO. | GAO-17-63

GAO

Good Practices to Implement and Sustain ERM

1) Leaders guide and sustain ERM strategy
2) Develop a risk-informed culture to ensure all employees can effectively raise risks
3) Integrate ERM capability to support strategic planning and organizational performance management
4) Established a customized ERM program integrated into existing agency processes
5) Continuously manage risks
6) Share information with internal and external stakeholders to identify and communicate risks

GAO

1) Leaders Guide and Sustain ERM Strategy

- **What:** Implementing ERM requires the full engagement and commitment of senior leaders, supports the role of leadership in the agency goal setting process, and demonstrates to agency staff the importance of ERM.
- **How:**
  - designate an ERM leader or leaders
  - commit organization resources to support ERM, and
  - set organizational risk appetite

Selected Leadership Examples

National Institute of Standards and Technology (NIST) Surveyed Leaders' Views of Risk Appetite

Office of Federal Student Aid (FSA) Committed Resources to Support ERM

Transportation Security Administration (TSA) ERM Process Is Led by a Chief Risk Officer and Senior-Level Executive Risk Steering Committee

NIST Risk Appetite Scale

Rating	Risk Taking Philosophy	Tolerance for Uncertainty How willing are you to accept uncertain outcomes, whether positive or negative?	Choice When faced with multiple options, how willing are you to select an option that puts this objective at risk?	Trade-Off How willing are you to trade off this objective against achievement of other objectives?
5 – Open	Will take justified risks	Fully anticipated	Will choose option with highest return; accept possibility of failure	Willing
4 – Flexible	Will take strongly justified risks	Expect some	Will choose to put at risk, but will manage the impact	Willing under certain conditions
3 – Cautious	Preference for safe delivery	Limited	Will accept if limited, and heavily out-weighed by benefits	Prefer to avoid
2 – Minimalist	Intentionally conservative	Low	Will accept only if essential, and limited possibility/extent of failure	With extreme reluctance
1 – Averse	Risk avoidance is a core objective	Extremely low	Will select the lowest risk option, always	Never

2) Develop a Risk Informed Culture

- **What:** Developing an organizational culture to encourage employees to identify and discuss risks openly is critical to ERM success.
- **How:**
  - encourage employees to discuss risks openly
  - train employees on ERM approach
  - engage employees in ERM efforts, and
  - customize ERM tools for organizational mission and culture.

Selected Risk Informed Culture Examples

HUD ERM Training Emphasized Culture Changes Needed to Raise Risks

Department of Commerce Defined Roles and Responsibilities Across the Agency to Build a Risk Management Culture and Guide Its ERM Process

TSA Sponsored Several Programs to Raise Risk Awareness Among Employees

NIST Adapted the Commerce ERM Framework to Reflect Lab Safety Vocabulary Appropriate to Its Culture

TSA Office of the Chief Risk Officer Programs to Increase Risk Awareness

1) Sponsored a risk community of interest open to any employee in the organization and has hosted speakers on ERM topics.
2) Created a risk lexicon, so that all staff involved with ERM would use and understand risk terminology similarly.
3) Established a vulnerability management process for offices and functions with responsibility for identifying or addressing security vulnerabilities.
   - helps raise risks from the bottom up so that they receive top level monitoring,
   - centralizes tracking of vulnerability mitigation efforts with the CRO,
   - provides executive engagement and oversight of enterprise vulnerabilities.
4) Established ERM Liaisons, senior-level official, in each program office.
5) Sponsored training on risk-based decision-making, risk assessment, and situational awareness.

GAO

3) Integrate ERM Capability to Support Strategic Planning and Organizational Performance Management

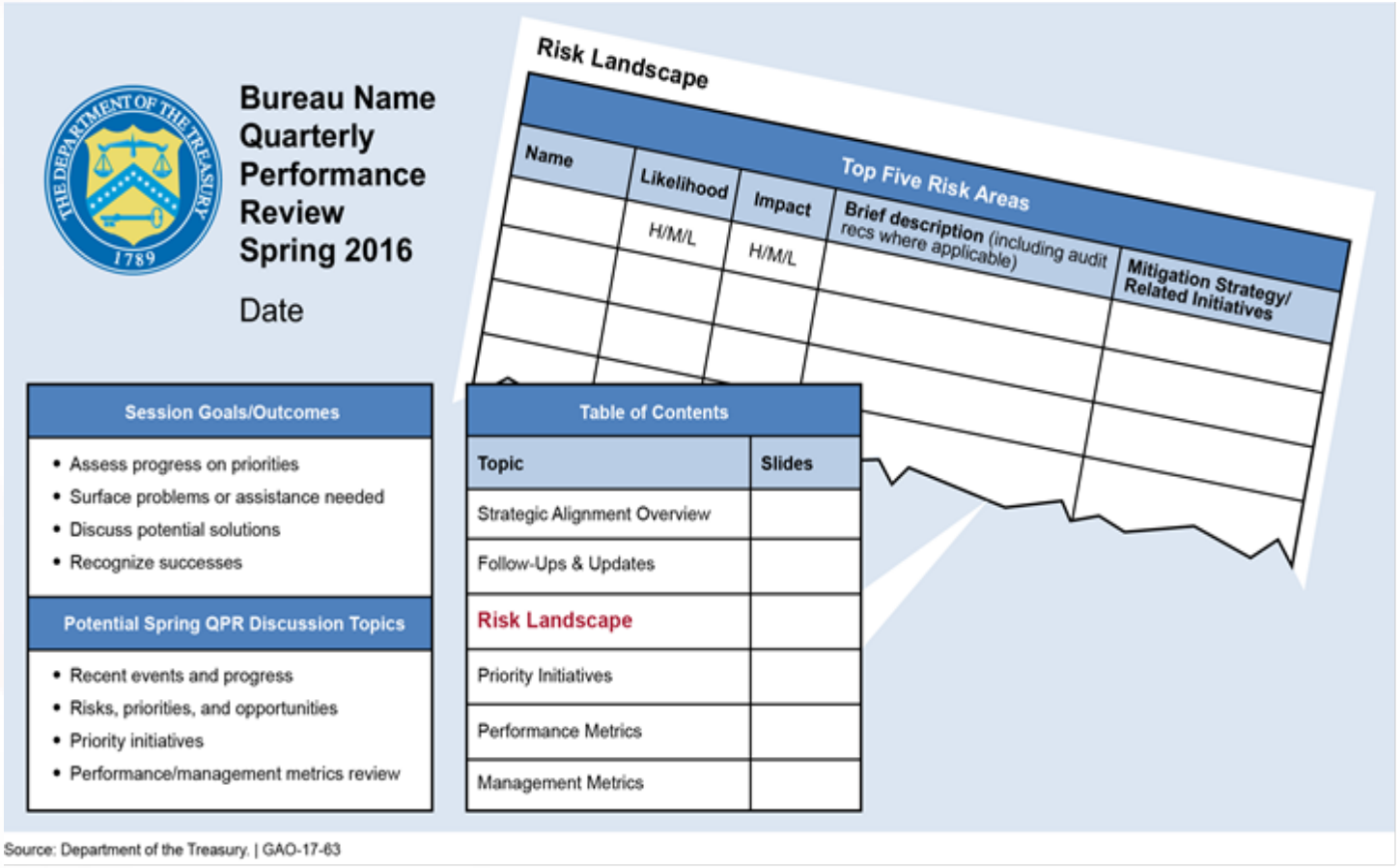
- **What:** Integrating the prioritized risk assessment into strategic planning and organizational performance management processes helps improve budgeting, operational, or resource allocation planning.
- **How:**
  - incorporate ERM into strategic planning processes, and
  - use ERM to improve information for agency decisions.

Selected Strategic Planning and Performance Management Examples

Department of the Treasury Used Risk Discussions in Quarterly Performance Reviews

Office of Personnel Management Builds Agency View of Risk into Decision Making and Organizational Performance Management Reviews

Department of the Treasury Quarterly Performance Review



Source: Department of the Treasury. | GAO-17-63

GAO

4) Establish a Customized ERM Program Integrated into Existing Agency Processes

- **What:** Customizing ERM helps agency leaders regularly consider risk and select the most appropriate risk response that fits the particular structure and culture of an agency.
- **How:**
  - design an ERM program that allows for customized agency fit,
  - develop a consistent, routinized ERM program, and
  - use a maturity model approach to build an ERM program.

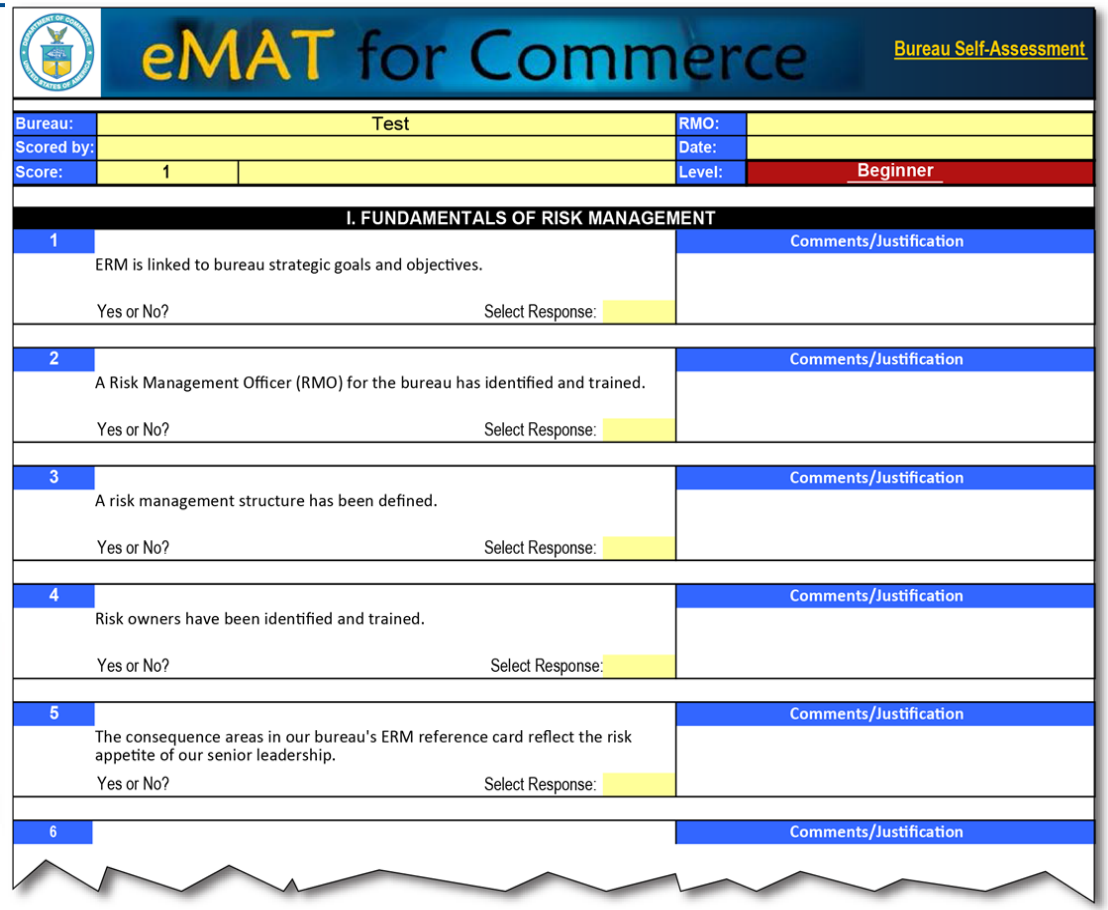
Selected Customized ERM Program Examples

TSA Risk Taxonomy Promotes a Consistent Approach to the Risk Review Process

FSA Customized Its Approach to Designing and Implementing ERM

Commerce Designed an Assessment Tool for Its Bureaus to Determine Their ERM Maturity

Commerce Maturity Assessment



eMAT for Commerce — Bureau Self-Assessment

Bureau:	Test	RMO:	
Scored by:		Date:	
Score:	1	Level:	Beginner

I. FUNDAMENTALS OF RISK MANAGEMENT

1	ERM is linked to bureau strategic goals and objectives. Yes or No? Select Response:	Comments/Justification
2	A Risk Management Officer (RMO) for the bureau has identified and trained. Yes or No? Select Response:	Comments/Justification
3	A risk management structure has been defined. Yes or No? Select Response:	Comments/Justification
4	Risk owners have been identified and trained. Yes or No? Select Response:	Comments/Justification
5	The consequence areas in our bureau's ERM reference card reflect the risk appetite of our senior leadership. Yes or No? Select Response:	Comments/Justification
6		Comments/Justification

Source: Department of Commerce. | GAO-17-63

5) Continuously Manage Risks

- **What:** Conducting the ERM review cycle on a regular basis and monitoring the selected risk response with performance indicators allows the agency to track results and impact on the mission, and whether the risk response is successful or requires additional actions.
- **How:**
  - track and monitor current and emerging risks.

Continuously Manage Risk Examples

HUD PIH Uses Risk Dashboards to Monitor Risks

PIH Key Risk Indicators

Source: Department of Housing and Urban Development Office of Public and Indian Housing. | GAO-17-63

GAO

6) Share Information with Internal and External Stakeholders to Identify and Communicate Risks

- **What:** Sharing risk information and incorporating feedback from internal and external stakeholders can help organizations identify and better manage risks, as well as increase transparency and accountability to Congress and taxpayers.
- **How:**
  - incorporate feedback on risks from internal and external stakeholders to better manage risks, and
  - share risk information across the enterprise.

Selected Share Risk Information Examples

Internal Revenue Service (IRS) Uses a Decision-Making Tool that Includes Input from Stakeholders Across the Enterprise

National Aeronautics and Space Administration and National Oceanic and Atmospheric Administration Use A Memorandum of Understanding to Share Accountability and Ownership for Risks from a Shared Satellite Program

IRS Risk Acceptance Form and Tool

Decision Making Framework
Risk Acceptance Form and Tool (RAFT)

Purpose: The purpose of this form is to provide a consistent framework for the Service that can be leveraged within a unit's existing governance or management approval processes to clearly document business decisions in the context of risk appetite and /or acceptance. This document can be used in various ways, including the following: 1) a framework to assess various options in making decisions for achievement of objectives, 2) a guide to articulate rational behind those decisions within the context of risk appetite, and 3) a documentation trail to support these business decisions.

Name/Title of RAFT	Date RAFT created/revised

Business Operating Division	Functional Operating Division	Special Unit (if applicable)

Office *(if applicable)*

External stakeholders affected

Objective *(Provide a brief problem statement, challenge, and/or the opportunity)*

Background *(Provide a summary of the background of the situation that the organization is facing and other relevant facts)*

Assessment and rationale

Decision or proposed decision *(Provide a brief overview of the decision)*

Description of risk acceptance *(Provide a description of the risk that is being accepted as a result of the assessment to articulate risk appetite. Consider what exposures result from the decision.)*

Additional monitoring

Source: Department of the Treasury and Internal Revenue Service. | GAO-17-63

GAO

Thoughts on Strategic Foresight Tools and ERM

- Strategic foresight is the practice of systematically identifying changes in the environment and the potential futures associated with those changes using a range of qualitative and quantitative methods, such as historical analysis, environmental scanning, alternate futures, trend analysis, and scenario planning, among others.
- These methods can be used to identify uncertainties (risks) in the internal and external environment that may impact organizational goals and objectives.
- Strategic foresight offers a range of tools to support an organization's strategic planning and ERM capability, particularly the process of identifying, assessing, and making decisions regarding long-term risks and opportunities.

GAO

Thoughts on Strategic Foresight Tools and ERM cont'd

- Strategic foresight methods are useful when designing an ERM capability and as a means of maintaining an ongoing understanding of an organization's risk.
- These methods can provide agency employees with a strategic, systematic way to think about and describe complex external and internal contexts. For example, it is important to evaluate and understand both the internal and external context of the organization before designing and implementing a framework for managing risk.

Thoughts on Strategic Foresight Tools and ERM cont'd

- Understanding the external context of an organization may include an analysis of social, economic, environmental, technological, or other factors, the key drivers and trends that may impact the organization's objectives or perceptions of stakeholders.
- An analysis of the internal context of an organization may include a review of governance structures, roles, and policies within an organization, the capabilities in terms of resources and knowledge, or culture, among other factors.
- As ERM capabilities mature, strategic foresight methods such as scenario planning, alternate futures, and trend analysis may help agencies identify unknown risks and opportunities as well as develop strategies to address those risks and take advantage of opportunities.