AFERM

Association for Federal Enterprise Risk Management

The CFO Council

Playbook - Enterprise Risk Management

May 28, 2021 | 12:00 – 1:30 PM

Agenda

- Opening Remarks
- Panelist Introductions
- Administrative

AFERM
Association for Federal
Enterprise Risk Management

Key Takeaways from ERM Playbook 2.0

1 **Maturity Model**

The model provides a tool for agencies to **continually self-assess ERM program maturity**, including related processes, governance, and value to the enterprise.

2 **Risk Appetite**

While there are several ways to approach risk appetite, any approach should consider **how tradeoffs are evaluated**, how it **applies in operational settings**, and how it **informs decision-making** up and down the organization.

3 **Integration with Management Processes**

Successful integration of ERM into agencies' day-to-day decision-making and management practices enables agencies **to leverage opportunities for accepting, reducing, sharing, pursuing or avoiding risk** that ultimately results in more resilient, effective, and efficient government programs.

4 **Cybersecurity**

This section provides a foundation in cybersecurity and information security basics and gives recommendations and best practices for consideration in **integrating cybersecurity and information security risk management** with broader agency ERM practices.

AFERM
Association for Federal Enterprise Risk Management

Alice Miller
Chief Risk Officer
U.S. International Development Finance Corporation

AFERM
Association for Federal
Enterprise Risk Management

Maturity Model

The new Playbook includes a federal government ERM maturity model which was developed by an interagency group and has been being "piloted" by a number of agencies. This model was developed to reflect the particularities of implementing ERM in a federal government setting and is scalable for use by both smaller and larger agencies.

Five Key Takeaways

+ OMB Circular No. A-123 instructs agencies to take a maturity model approach to the development and implementation of their ERM programs; this **model supports that mandate**.
+ The model **facilitates flexibility in implementing ERM programs**, does not prescribe how to implement an ERM Program, and is not meant to be a compliance or audit "checklist."
+ The model provides a tool for agencies to **continually self-assess ERM program maturity**, including related processes, governance, and value to the enterprise.
+ The approach facilitates an **integrated, holistic consideration** of risks and opportunities.
+ Doing a **baseline maturity model assessment**, then annual assessments thereafter can help agencies to better communicate about progress and areas for improvement.

AFERM
Association for Federal Enterprise Risk Management

Jason Leecost
Director, Officer of Enterprise Risk
Ginnie Mae

AFERM
Association for Federal
Enterprise Risk Management

Risk Appetite

While there are several ways to approach risk appetite, any approach should consider how tradeoffs are evaluated, how it applies in operational settings, and how it informs decision-making up and down the organization.

Five Key Takeaways

+ Agencies may take more or less risk to achieve objectives even if their appetite is not defined, but appetite is only useful if it can be **cascaded down, interpreted, and utilized by employees** at all levels within the agency.

+ Clear and practical risk appetite statements **provide guidance on the amount of risk that is acceptable** when pursuing objectives, making risk-informed decisions, and avoiding unexpected surprises.

+ Risk appetite implementation needs to **translate statements into operational levels**, including how appetite and tolerance will be measured using available metrics.

+ Agencies will need to adopt their own approaches to establishing and updating risk appetite, but any approach should consider **which tradeoffs are necessary and whether that tradeoff is acceptable.**

+ Risk appetite provides a **guidepost for prioritizing** which risks to respond to first, which require further action, and importantly, whether the risk response will require additional resources or other budget considerations.

AFERM
Association for Federal Enterprise Risk Management

Karen Weber
Deputy Chief Risk Officer
Department of the Treasury

AFERM
Association for Federal
Enterprise Risk Management

Integration with Management Practices

The original Playbook only provided a high-level summary of how ERM should integrate with other management practices. The updated Playbook describes in a more in-depth way how ERM can work with strategic planning, performance, budget, and internal controls.

Five Key Takeaways

+ Last July, OMB updated A-11 to emphasize that ERM should be **included in agency's strategic planning, performance, and budget discussions**. These changes try to explain how that can be done.

+ During development of the Strategic Plan, **considering the future and its associated risks** in the early stages of the process will help the agency better align the management of risks with the organization's overall mission, goals, and objectives

+ The Strategic Objective Review process can be a very effective way to **identify opportunities and manage risks to performance** for those risks related to achieving an agency's mission.

+ Clear, data-rich information on an agency's significant risks can help agency leadership make **better risk-based decisions for internal budget allocation**- to pursue risks, seek additional funds and make trade-offs.

+ Updated A-123 Appendix A expands internal controls to all reporting objectives. By working with ERM and understanding the risks, internal controls offices can determine **where inaccurate, unreliable, or outstanding reporting** could significantly impact the agency's ability to accomplish its mission and performance goals or objectives.

AFERM
Association for Federal Enterprise Risk Management

Nahla Ivy
Enterprise Risk Management Officer
National Institute of Standards and Technology

AFERM
Association for Federal
Enterprise Risk Management

Cybersecurity

The updated Playbook addresses the integration of cybersecurity and information security risk management with agency ERM. This is an emerging area of need within federal agencies, yet many are still figuring out how to tackle it. Cybersecurity and information security risks remain among the top risks for many federal agencies (AFERM 2020 Survey).

Five Key Takeaways

+ **Addresses commonality in terms** across the domains of cyber and information security risk management and agency enterprise risk management programs. Intended to be a useful guide for both ERM and IT practitioners.

+ Based on the foundations and tenets of the National Institute of Standards and Technology (NIST) information security and cybersecurity publications, frameworks, and best practices; this **extends to privacy risk and supply chain risk management**.

+ Includes **best practices collected by agencies** based on experiences in integrating these practice areas, including successes and lessons learned.

+ Recommends expanding relationships and methods to enable both **vertical and horizontal communications paths** (translation of risks between organizational levels; supporting decisions at the enterprise level).

+ Addresses a long-standing challenge related to perceived overreach of FISMA audits into audits of agency ERM programs. Recent revised FISMA metrics address this by **drawing additional lines**.

AFERM
Association for Federal Enterprise Risk Management

Contributors

Enterprise Risk Management Playbook 2.0

Karen Weber	Update Chair	Department of the Treasury (Treasury)
William Bowman	Editor/ Working Group	Veterans Health Administration
Jill Lennox	Editor/ Working Group	Federal Deposit Insurance Corporation (FDIC)
Alex Wilson	Editor	Treasury
Piyavuth Bhutrakarn	Working Group	Internal Revenue Service (IRS)
Julie Chua	Working Group	Department of Health and Human Services (HHS)
Christopher Calfee	Working Group	FDIC
Maria Cruz	Working Group	U.S. Agency for International Development (USAID)
Karen Francis	Working Group	Federal Retirement Thrift Investment Board
Robin Funston	Working Group	Department of Justice (Justice)
Lori Giblin	Working Group	Millennium Challenge Corporation
Itzel Gonzalez	Working Group	National Institutes of Health (NIH)
Kim Isaac	Working Group	Cybersecurity and Infrastructure Security Agency
Nahla Ivy	Working Group	National Institute of Standards and Technology (NIST)
Eleni Jernell	Working Group	Nuclear Regulatory Commission
Jonathan Jones	Working Group	HHS
Daniel Kaneshiro	Working Group	Office of Management and Budget (OMB)
Daniel Lagraffe	Working Group	Department of Energy
Nancy Laurine	Working Group	USAID
Jacob Lee	Working Group	Department of Interior
Jason Leecost	Working Group	Ginnie Mae
Adam Lipton	Working Group	OMB
Lydia Lourbacos	Working Group	Bureau of Safety and Environmental Enforcement
Mary Marvin	Working Group	Social Security Administration
Curtis Masiello	Working Group	Department of Defense (Defense)
Curtis McNeil	Working Group	Architect of the Capitol
Alice Miller	Working Group	U.S. International Development Finance Corporation
Reginald Mitchell	Working Group	USAID
James Moore	Working Group	Office of the Comptroller of the Currency (OCC)
Thomas Moschetto	Working Group	Treasury
Nnake Nweke	Working Group	U.S. Agency for Global Media (USAGM)
Andrea Peoples	Working Group	Small Business Administration
Victoria Pillitteri	Working Group	NIST
Stephen Quinn	Working Group	NIST
Ahmad Rasuli	Working Group	Treasury
Melissa Reynard	Working Group	IRS
Nicole Rohloff	Working Group	NIH
Marianne Roth	Working Group	Consumer Financial Protection Bureau
Liz Ryan	Working Group	Export Import Bank
Christopher Smith	Working Group	Defense
Lenora Stiles	Working Group	Treasury
Kevin Stutts	Working Group	FDIC
Angelina Sulaka	Working Group	USAGM
Fahiem Usman	Working Group	Treasury
Joshua Vogel	Working Group	General Services Administration
Derrick Ward	Working Group	Transportation Security Administration
Debra Williams	Working Group	Justice
Jing Williams	Working Group	HHS
Montrice Yakimov	Working Group	FDIC
Jane Yang	Working Group	Pension Benefit Guarantee Corporation
William Rowe	Contributor	OCC
Neil Starzynski	Contributor	Department of Labor

AFERM

Association for Federal
Enterprise Risk Management

Questions