2017 ERM Workshop:

Beyond Compliance, Driving Organizational Value

June 7, 2017

AGA®

AFERM
Association for Federal Enterprise Risk Management

ACKNOWLEDGMENTS

AGA

Ann M. Ebberts, Chief Executive Officer

Susan Fritzlen, Chief Operating Officer

Anna Schumann, Communications Manager

AFERM

Sallyanne Harper, President

Thomas Holland, Programs Committee Chair

In Appreciation

Special thanks to all of the sponsors (see page 7) for facilitating and capturing the round-table discussions from which this report was produced.

Additional thanks for the writing of this executive summary to the following contributors:

Sheri Francis, TFC Consulting

Chris Hare, Grant Thornton

Thomas Holland, PwC

Rosa Milani, PwC

Idalia Moore, PwC

Stephen Watson, TFC Consulting

AGA is *the* member organization for financial management professionals in government. We lead and encourage change that benefits our field and all citizens. Our networking events, professional certification, publications and ongoing education help members build their skills and advance their careers.

AFERM is the only professional association solely dedicated to the advancement of enterprise risk management (ERM) in the federal government through thought leadership, education and collaboration. AFERM provides programs and education about benefits, tools and leading practices of federal ERM and collaborates with other organizations and stakeholders to encourage the establishment of ERM in federal departments and agencies.

EXECUTIVE SUMMARY

AGA and the Association for Federal Enterprise Risk Management (AFERM) hosted a workshop for more than 150 federal professionals interested in enterprise risk management (ERM) on June 7, 2017. The purpose of the workshop was to provide a forum for federal ERM professionals to share progress and best practices related to using ERM to drive organizational value. The workshop focused on providing an overview and small group discussion about three critical aspects of ERM:

1. ERM implementation and developing the agency risk profile;
2. the relationship between ERM and internal controls; and
3. using ERM to enable better risk management and decision making within the agency.

The tone of the workshop was set by Ken Phelan, chief risk officer (CRO), U.S. Department of the Treasury; and Mark Reger, deputy controller of the United States, Office of Management and Budget (OMB), who presented an overview of ERM implementation in the federal government. Presentations by federal CROs and risk managers provided the individual session overviews, including lessons learned and relevant "on the ground" experiences, leading into the facilitated small-group discussions.

For the first session, Tom Brandt, CRO for the Internal Revenue Service (IRS) and Larry Koskinen, CRO from the U.S. Department of Housing and Urban Development (HUD) discussed developing risk profiles and evolving the enterprise risk assessment process over time. For the second session, Karen Hardy, deputy CRO and director of the risk management division at the U.S. Department of Commerce, presented on how ERM and internal controls are mutually beneficial, but different. For the final session, Jennifer Main, chief financial officer (CFO) for the Centers for Medicare and Medicaid Services (CMS), shared examples about using ERM for better decision making.

> An important early step for ERM is to define risk-rating criteria to be used consistently.

Each presentation was followed by facilitated round-table discussions on the topic, during which knowledge, agency experiences, ideas and best practices were shared. This report captures many of the key ideas and practices indentified during these discussions, so they can be shared among the wider federal ERM community. We extend our thanks to the presenters, workshop participants, and corporate sponsors who facilitated the sessions and captured notes from the event.

Developing a Risk Profile and Evolving Your Enterprise Risk Assessment Process Over Time

Developing an enterprise risk profile is an important foundational step for ERM at any agency. Developing and maintaining an enterprise risk profile provides an agency the opportunity to understand and respond to the greatest risks to the agency's ability to achieve its strategic goals, in the context of the current internal and external environments. With the July 2016 release of the updated OMB Circular No. A-123, federal agencies are required to develop and maintain a risk profile to "provide a thoughtful analysis of the risks an agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks."

The group discussions for this session focused primarily on three topics:

- challenges to obtaining the information necessary to develop a risk profile and ways to overcome those challenges;
- techniques that have worked well for developing a risk profile; and
- how to make sure that the risk profile is something used by the agency to better inform decision making and resource allocation.

Multiple participants discussed agency culture as well as the existence of organizational silos as two challenges to obtaining risk information. ERM requires open and candid discussions regarding risks; however, some organizations find risk-based dialog is often suppressed to maintain the status quo and to avoid risk ownership. Obtaining employee buy in has also proven to be a challenge for many organizations, because the bigger picture — or value add — of the

> It is critical that the process encompasses the full spectrum of risk types, and does not overly focus on one type of risk, such as financial risk, because of where the coordinating function is located in the agency.

activity can be unclear, especially to staff-level employees. If not carefully managed, and structured properly, these efforts can result in employees viewing the additional risk management activities as a check-the-box compliance exercise.

Gathering and communicating enterprise-wide risks is challenging because many employees are so focused on their respective departments that it can result in a silo mentality and make it challenging for employees to understand risks from an enterprise perspective, participants said. The silo mentality, coupled with the absence of common risk terminology and frameworks across departments in some agencies causes confusion when identifying and aggregating risks cross-agency. One challenge mentioned was that similar risks are rated against different criterion, thus resulting in different impact scores and making it difficult to develop a reliable prioritization of the risks. An important early step for ERM is to define risk-rating criteria to be used consistently.

The participants discussed the importance of creating an environment in which employees feel comfortable and even incentivized to discuss and escalate risks, without fear of retaliation. Some agency leaders hold regular meetings to discuss progress made, responding to top risks and reminding all employees of their role in ERM; these meetings have helped encourage people to share risk information more openly. Some groups discussed performing an environmental scan (e.g., SWOT or PESTLE analysis) to get employees thinking about risks that may be appropriate for the risk profile. Also, some groups emphasized that leadership should gather risk profile information, not only from the top, but also from the staff levels of the agency. One way to do this is to leverage ERM liaisons to facilitate working group discussions and participate in steering committees to provide input on the risks their organization faces. Many participants stated it was critical to compose clear, concise and logical risk statements. For example, groups discussed using an "if/then" format, in which the "if" portion describes the risk event or threat, and the "then" portion describes the event's impact or result to the agency.

When discussing leveraging the risk profile for budget and strategic planning, some groups discussed the importance of aligning risks to strategic goals and objectives. Certain agencies found this approach enabled management to identify which strategic objectives had the highest levels of associated risk. This has also helped agencies make strategic investments toward mitigating risks to strategic objectives, and has helped justify funding for resources in the annual spending plan.

Groups acknowledged that the risk profile is a living document that should be continuously reviewed and updated as appropriate, and that an agency's approach to enterprise risk assessment should similarly evolve over time as the agency's ERM and risk management capabilities evolve.

ERM and Internal Controls: Different but Mutually Beneficial

OMB Circular No. A-123 emphasizes the importance of having a coordinated approach to ERM and internal controls that is integrated into existing business activities as an integral part of managing an agency. For many agencies, their internal control functions and efforts are well established and their ERM efforts are in much earlier stages of development. The challenge agencies face is determining the level of coordination between the various elements of their ERM and internal control programs that will best support the achievement of agency objectives and the overall mission.

The group discussions for this session focused primarily on the following topic areas:

- where ERM leadership resides within the organization;
- areas in which it is beneficial for ERM and internal control efforts to be coordinated; and
- skills that are useful for both ERM and internal controls implementation.

Agency establishment of ERM has taken a variety of shapes and forms. Initially, some agencies defaulted ERM responsibilities to the

CFO or financial management office, given that responsibility for Circular No. A-123 compliance has typically resided with finance. Other agencies have established a chief risk office or assigned risk management responsibilities to existing offices such as the chief operating office or the office of strategic planning. Some agencies have dispersed risk management responsibilities across different components and divisions. Generally, ERM was not discussed as being combined into existing internal control or compliance programs; rather, it was discussed as its own effort. Multiple groups noted that no matter where ERM sits, it is critical that the process encompasses the full spectrum of risk types, and does not overly focus on one type of risk, such as financial risk, because of where the coordinating function is located in the agency. Multiple groups also emphasized the importance of having a senior-level official in charge of ERM, and specifically an individual that can effect change at the agency. It was also discussed that having the head of ERM be a career person, rather than a political appointee, can help ensure continuity of ERM efforts through an administration change.

One challenge with ERM implementation can be ensuring coordination with existing internal control and compliance programs where appropriate. Agencies also find it challenging to implement ERM without key leadership buy-in, including designating how ERM is to connect with existing internal control and compliance programs. Some participants felt that ERM and the internal control functions were not communicating as well as they could be and that there are more opportunities for both groups to leverage information from each other. Participants also recognized that the solution is not to combine the function, as that can often create its own set of challenges. Another challenge participants discussed was how to measure and monitor ERM performance and its impact on the agency.

Discussions also surfaced that there is some overlap in skill sets required for ERM and internal controls. It was also mentioned that some agencies are cross-training their ERM and internal control resources. This enables the ERM and internal control teams to have a better understanding of the synergies as well as the differences between ERM and internal control efforts, to better coordinate and support the agency.

Regardless of where ERM resides in the organization, ERM and internal controls functions can work together to align their mutual objectives to cost-effectively enable the agency to manage its risks and help it achieve its objectives and fulfill its mission.

Using ERM for Better Decision Making

How ERM is integrated within an agency can have a great effect on an organization's budget and strategic planning for the future. Effective ERM provides timely and useful information to inform strategic planning and resource allocation. Transparency up, down and across an agency is a key element to positively influencing behaviors, and enabling more informed decision making at all levels. To enable this type of transparency, it is critical for senior leaders within the agency to set the tone, including by encouraging individuals at all levels to share information and by setting a good example and sharing information with the lower levels of the organization. ERM can assist leadership and their decision-making abilities by enhancing the flow of information, increasing management accountability, and helping the agency think prospectively about risks and respond accordingly.

While the group discussions covered a range of good practices and challenges, the discussions were primarily grounded in three areas:

- how ERM is being integrated within each agency;
- effective techniques for breaking down silos and sharing information; and
- ways in which ERM can be a tool for emphasizing management accountability and performance.

When discussing integrating ERM into an agency's structures and processes, multiple groups noted how critical it is to first understand the existing risk management activities within the agency and to try to build upon those as much as possible when

> Having committees with a healthy balance of career leaders and political appointees helps enable the committee to continue to operate with minimal interruption through an administration change.

designing an ERM program. One group noted that the CRO, or other head of ERM, needs to be viewed as someone who helps make people's lives better, and provides frequent and consistent communication about ERM's intent. Another group remarked on the importance of ensuring that risks are owned by the various programs, and not seen as owned by the ERM function.

Most groups discussed having established an executive committee or council that reviews and discusses enterprise risks. Many participants also discussed the use of working groups with representation across programs or units to share information and conduct risk analysis. In some cases, the working groups decide which risks to elevate to the enterprise level and add to the agency's enterprise risk profile. One group noted that having committees with a healthy balance of career leaders and political appointees enables the committee to continue to operate with minimal interruption through an administration change. Having committees and work groups that span programs or units can help break down the silos that can be an impediment to effective ERM. Also, leveraging existing leadership meetings is a good practice, if the focus is compatible with what is needed from an ERM-related committee. One group noted that it was critical to understand who makes decisions (committees or individual leaders) within the organization and to use that understanding to inform the approach to ERM.

Several groups discussed other ways to break down silos and encourage information sharing. Participants noted that for people to be willing to share information outside of their group, they need to see the value of sharing it. Participants acknowledged that the CRO or ERM leader needs to take the initiative to share and collaborate as much as possible, in order to model the preferred behavior. Additionally, to help others see the value, it is important to communicate examples of how sharing information and collaborating across groups has led to better outcomes.

Multiple groups noted the importance of increasing the level of communication, including communication up, down and across the organization. Increased levels of communication will enable better decision making and help provide greater transparency for enhanced accountability and performance management. Participants discussed that it can be helpful to incentivize good risk management, including actively identifying and communicating risks. Participants noted that linking ERM with the strategy, budget and performance management processes can be an effective way to encourage the identification and elevation of risks and to enhance accountability and performance. One example provided was adding performance commitments or job requirements related to ERM or risk management, which helps enforce accountability throughout the agency for effective risk management. Assigning accountable officials at the risk and mitigation level is another way to enforce accountability for risk management throughout the agency.

It can be helpful to incentivize good risk management, including actively identifying and communicating risks.

While there are several techniques for integrating ERM into the key decision-making processes of the agency, agencies must determine an approach that works best with their existing culture to leverage the potential of ERM to enable better informed decision making at all levels and to enhance accountability.

Conclusion

Agencies progress at different rates with their ERM implementation. Some agencies are developing their first enterprise risk profile, while others have been maintaining a risk profile for a few years now and are more focused on fully integrating risk management at the enterprise level with the agency's strategic planning, budget, and performance management processes. Regardless of where agencies are in the ERM implementation process, it is clear from the discussions that agencies are leveraging ERM as a tool to enable better informed decision making, enhance resource allocation, inform strategy, and enable the agency to deliver on its mission efficiently and effectively.

2017 ERM Workshop: Beyond Compliance, Driving Organizational Value

June 7 | 8 a.m. – 2 p.m. | Ronald Reagan Building & International Trade Center, Washington | 5 CPEs

Thank you to our sponsors for making this event possible:

CohnReznick

Crowe Horwath

Deloitte.

EY Building a better working world

Franklin & Turner Consultants and Certified Public Accountants

Grant Thornton

Kearney & Company

KGS

KPMG

MorganFranklin Consulting

pwc

tfc

Williams Adley

AGA

Co-hosted by AGA and AFERM

AFERM Association for Federal Enterprise Risk Management www.agacgfm.org