2018 ERM WORKSHOP

Beyond Compliance, Driving Organizational Value

April 16, 2018

AGA®

AFERM
Association for Federal
Enterprise Risk Management

ACKNOWLEDGEMENTS

AGA

Ann M. Ebberts, Chief Executive Officer

Susan Fritzlen, Chief Operating Officer

Lyndsay McKeown, Marketing & Graphics Manager

AFERM

Peggy Sherry, President

Sallyanne Harper, Past President

Thomas Holland, Programs Committee Chair

In Appreciation

Special thanks to the Planning Committee who made the workshop possible and to all of the sponsors (see page 9) 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:

Bert Nuehring, Crowe
Sarah Choi, Guidehouse
Sukriti Gujral, AFERM
Thomas Holland, Guidehouse
Tyler Krase, TFC Consulting

AGA is *the* member organization for government finance professionals. 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

On April 16, 2018, the Association of Government Accountants (AGA) and the Association for Federal Enterprise Risk Management (AFERM) held the second annual enterprise risk management (ERM) workshop with federal government professionals. This workshop provided an opportunity for over 150 professionals to hear ERM thought leadership from senior government leaders and discuss with their colleagues how ERM can, and is, driving organizational value and enhancing performance. The workshop focused on three key areas:

1. Enhancing ERM capability over time
2. Integrating ERM with strategy and performance
3. ERM and cybersecurity.

Mark Bussow, policy analyst at the Office of Management and Budget (OMB) and Chris Mihm, managing director at the Government Accountability Office (GAO) kicked off the workshop. During their presentation, they emphasized how OMB and GAO's partnership is advancing ERM in the federal government through guidance and regulation while understanding that each agency will have a different ERM journey.

The structure of the workshop included presentations for each of the key focus areas. For the first session, Marianne Roth, chief risk officer(CRO) at the Consumer Financial Protection Bureau (CFPB) and Yakisha Rahaman, senior advisor to the CFO at the Food and Drug Administration (FDA), discussed how enhancing ERM and risk management capabilities enables the evolution of ERM and related processes. The second session, led by Tom Brandt, chief risk officer for the Internal Revenue Service (IRS) and Kevin Long, strategy branch chief at the Federal Insurance and Mitigation Administration (FIMA), covered the benefits of integrating ERM with strategy and performance. The third and final session was led by Chip Fulghum, deputy undersecretary for management at the Department of Homeland Security (DHS), who discussed the mutually beneficial relationship between ERM and many cybersecurity processes and practices.

Each presentation was followed by facilitated discussions on the topic where knowledge, agency experiences, ideas and best practices were shared in small groups. This report captures many of the ideas and innovative practices identified during these discussions so that they can be shared across the wider federal ERM community.

Session 1: Enhancing ERM Capability Over Time

With the release of updates to OMB Circular A-123 in July 2016 and additional updates specific to Appendix A released in June 2018, our understanding of ERM and its application across the federal government continues to evolve. The updates to OMB Circular A-123 dictates that all agencies must prepare a complete risk profile annually to inform changes to strategy, policy, operations and the president's budget. Since the July 2017 delivery of agency initial risk profiles, each consecutive iteration should continue to demonstrate further development and integration with all aspects of the agency or department.

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

- Current identity of ERM in the government
- Development of a value proposition for ERM activities
- Using growth along maturity models to drive the creation of quantifiable performance management metrics

Many of the initial discussions focused on the state of ERM at the participants' respective agencies. Many participants felt that while their exposure to the ERM concept and ERM activities at their agencies is increasing, the maturity levels and degree of use varies from agency to agency and between silos within an agency. The participants thought that this could be attributed to decentralized operations and varying leadership commitment and opinions on the effectiveness of ERM.

The participants noted that obtaining buy-in from stakeholders at all levels of the organization is a common challenge to maturity of ERM programs. Creating a value proposition is a practice used by many agencies to tie ERM activities to organizational value. Agencies pointed to the transparency of the risk environment between silos of an agency as an effective way to break down impediments to collaborative strategic planning. The participants also highlighted the significance of assessing the value of ERM activities not only in terms of mitigating risks, but also for potential opportunities. This dual-concept approach gives a clearer picture for organizational decision makers and enables all employees to understand the impact their decisions and actions have on the organization.

Participants also discussed the need for changes at the top to encourage more promotion of the value and further integration of ERM into day-to-day activities. ERM should be included as part of strategic planning, budget formulation and performance management discussions. Several participants felt their agencies benefitted from appointing a CRO to champion these discussions among leadership and throughout the organization.

Since many of the government's operations are qualitative in nature, it is often difficult to quantify performance measures that can be analyzed as part of strategic planning. One agency noted a challenge related to quantifying human resources performance due to the limited impact the department's operations has on the financial statements. Many agencies noted utilizing a maturity model enabled them to better assess their program's maturity and provide additional data for decision making and strategic planning.

Throughout the conversation, group members wanted to know how to properly measure progress throughout the maturity matrix and how to apply those metrics to improve their approach to performance management. One method discussed measures the probability, severity and coverage of enterprise risks into a quantifiable rating. This method supports a logical approach to strategic planning by properly prioritizing assessment of internal controls at the program level to help mitigate risks and improve critical processes. Analysis performed on the assessment results creates valuable data for organizational decision makers to understand the progress of their process improvement, internal control and ERM efforts. Some participants noted that this approach allowed them to more efficiently allocate resources across the organization.

Session 2: Integrating ERM with Strategy and Performance

Recent updates to the COSO ERM Framework and ISO 3100 emphasize the importance of integrating ERM with strategy and performance. Additionally, the August 2017 release of OMB Circular A-11 calls for federal agencies to utilize the annual strategic review process to make risk-aware decisions and coordinate its analysis of risk using ERM . OMB Circular A-11 also encourages federal agencies to conduct thoughtful analysis of the risks an agency faces in achieving its strategic objectives. Integrating ERM in an organization can enhance performance and improve strategic decision making.

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

- How is performance measured and how is risk considered as a part of measuring performance
- Risk and performance reporting within the organization
- Methods used to gain acceptance and shift the culture around risk-enabled performance management

Each federal agency has a risk appetite that adheres to its strategic aspirations. By outlining an agency's strategic vision as part of the strategic review process, the agency will be able to determine the total risk the organization is willing to undertake (risk appetite) and the total amount of uncertainty an organization is prepared to accept (risk tolerance).

Participants shared examples as to how their agencies defined risk in terms of activities that needed to occur for the needle to move in the right direction. Performance metrics in these scenarios were evaluated based on the ability to meet identified targets. When the goals were not achieved, the agencies would reassess the previously identified risks and adjust the existing risk tolerances accordingly.

Methods to measure agency performance include reviewing thresholds as part of a triannual review, monthly dashboard certifications and increased accountability at the associate director level for meeting performance targets. Participants discussed the importance of integrating identified risks into an agency's annual performance plan as a technique to improve the organizational culture.

All participants agreed that accountability, both bottom-up and top-down, would enable organizations to embrace effective risk management procedures. By not taking ownership of potential risk areas, the organization is ill-equipped to prepare for cases of severe risk and may need to resort to crisis management. Improper and undeveloped reporting structures prevent pertinent risk communications from being directed to those individuals with the authority to remediate the identified threat.

Participants also discussed the importance of installing a non-political appointee as CRO to maintain independence. Others added that the CRO should report directly to a senior governance committee, such as the audit committee, rather than being housed under the CFO as this will streamline the ability to address emerging issues. In addition, by not reporting directly to the CFO, the number of financial statement risks reported to senior leadership may decrease and will allow for a more robust dialogue around strategic and operational threats to the organization and for a broader, cross-agency risk outlook.

Lastly, a few participants encouraged better communication between divisions within the organizations to help the organization succeed. Members from the risk, financial, procurement and strategy offices should convene and discuss a united vision and strategy for the upcoming year.

Session 3: ERM and Cybersecurity

Cybersecurity knowledge varied among the participants. A small number noted that cybersecurity is discussed widely and thoroughly within their organization. However, a majority agreed that cybersecurity is a segregated risk that is typically only discussed by the chief information officer (CIO) or chief information security officer (CISO) groups. Although many felt that cybersecurity is currently segregated, participants agreed that cybersecurity is an important and growing area of the organization and expressed interest in integrating cybersecurity risk management processes and ERM.

With integration in mind, this session focused on the following topics:

- Engaging employees in strengthening cybersecurity measures
- Mitigating cybersecurity risks
- Communicating cybersecurity risks throughout the organization
- Linking cybersecurity risk to the ERM strategy

Employee engagement plays a key role in creating a successful integration of cybersecurity and ERM. During a discussion on how an organization's leadership can engage employees in strengthening cybersecurity measures, one participant suggested hosting regular training sessions and incorporating scenario planning and real-life simulations. Currently, basic cybersecurity training is offered as an annual requirement for all employees and some agencies have recurring reminders such as phishing tests and security bulletins. Most agreed that current annual training is ineffective, especially if the information is not updated to reflect the current cybersecurity environment. Many participants agreed that training is provided more frequently to those directly involved in cybersecurity.

When discussing individual roles in mitigating cybersecurity risks within the organization, it was widely agreed that the CIO is responsible as the most prominent point of contact for cybersecurity. Many believed that other segments of the organization may lack the capability or insight to respond to a cybersecurity risk. However, some participants felt that every individual had a role in mitigating cybersecurity risk and the level of engagement varied depending on the role. For instance, a non-IT professional would play a role in mitigating cybersecurity risk by proper handling of confidential information, attending training and following cybersecurity guidelines and protocols. One participant noted that they have an IT Risk Committee within their organization, however, the committee usually focuses on procurement rather than cybersecurity risks.

All groups mentioned that cybersecurity risks are communicated throughout their organizations by generic emails and alerts, along with occasional intranet articles, cyber pop-ups and short reminders. One organization issues a quarterly newsletter to all employees with cybersecurity updates and another has an annual risk culture day that is attended by senior executives within the organization. Though communication occurs somewhat frequently among most of the organizations, there was a general consensus that communication could be improved and delivered more effectively and would ultimately play a large part in integrating cybersecurity and ERM. Currently, there is little information distributed among organizations on how to integrate cybersecurity and ERM. As previously mentioned, most participants expressed interest in integrating cybersecurity and ERM and those participants agree that the need for integration has been acknowledged within their organization. However, there has been no evidence of action by the organization to integrate.

Effectively linking cybersecurity risks to the ERM strategy is critical for a successful integration. Nearly every participant agreed that the agency CIO must be actively involved in the discussions around enterprise risks to accomplish this. The understanding and use of National Institute of Standards and Technology (NIST) standards, which were created to guide organizations in implementing a strong and resilient cybersecurity infrastructure, is a good starting point for linking cybersecurity to the ERM strategy. Many participants were not familiar with NIST standards because it has typically been viewed as guidance that applies only to IT professionals. An increase in awareness and understanding of NIST standards could speed up the timeline for cybersecurity and ERM integration.

Based on the table discussions and participant insight, most organizations are beginning to consider how their cybersecurity and ERM functions and processes can work together. The participants agreed that employee engagement, such as frequent training sessions and simulations, along with increased communication would be instrumental in developing a successful integration. Employee engagement activities will also be decidedly beneficial in identifying and mitigating cybersecurity risks by all individuals within the organization. Participants in the table discussions agreed that linking cybersecurity to the ERM strategy is the next step to ensuring better risk mitigation strategies.

Conclusion

The ERM journey is unique for each organization, but there are scenarios that are shared across all levels of the federal government. This ERM workshop provided a valuable opportunity for federal ERM practitioners to connect and speak with colleagues to share insights, experiences and lessons learned in ERM implementation. ERM implementation and maturity is at varying degrees across the federal government, but the interest and understanding is growing across organizations and across a broad range of disciplines. All workshop participants agreed on the importance of enhancing ERM capability over time, integrating ERM with agency strategy and performance and increasing coordination between cybersecurity and ERM efforts. It is clear from the discussions that effective ERM is a priority across the federal government and agencies are focused on getting the most from ERM to enable their agencies to deliver its mission efficiently and effectively.

Appendix: Participating Government Entities

Agency for International Development
Architect of the Capitol
Broadcasting Board of Governors
Consumer Financial Protection Bureau
Environmental Protection Agency
Export-Import Bank of the United States
Federal Housing Finance Agency
Federal Reserve Board
Federal Retirement Thrift Investment Board
General Services Administration
  - Office of Inspector General
Government Accountability Office
Millennium Challenge Corporation
National Archives and Records Administration
National Credit Union Administration
National Science Foundation
Office of Management and Budget
Office of Personnel Management
Pension Benefit Guaranty Corporation
Securities Exchange Commission
Small Business Administration
Smithsonian Institution
Social Security Administration
U.S. Coast Guard
U.S. Department of Agriculture
  - National Resources Conservation Service
  - Office of Rural Development
U.S. Department of Commerce
  - National Institute of Standards and Technology
  - National Oceanic and Atmospheric Administration
U.S. Department of Education
  - Federal Student Aid
U.S. Department of Energy
  -Federal Energy Regulatory Commission
Department of Health and Human Services
  - Centers for Disease Control and Prevention
  - Centers for Medicare and Medicaid Services
  - Food and Drug Administration
  - Health Resources and Services Administration
U.S. Department of Homeland Security
  - Federal Emergency Management Agency
  - Federal Insurance and Mitigation Administration
  - Transportation Security Administration
U.S. Department of Housing and Urban Development
U.S. Department of the Interior
U.S. Department of Justice
  - Bureau of Alcohol, Tobacco, Firearms and Explosives
  - Federal Bureau of Investigation
U.S. Department of Labor
U.S. Department of State
U.S. Department of the Treasury
  - Internal Revenue Service
  - Office of the Comptroller of the Currency
U.S. Department of Veterans Affairs
U.S. House of Representatives
Washington Metropolitan Area Transit Authority

Thank you to our Sponsors

11th Hour SERVICE
Changing Futures, One Hour at a Time

ARM
Active Risk Manager

CliftonLarsonAllen

CohnReznick

Crowe

Deloitte.

EY
Building a better working world

Grant Thornton

KEARNEY& COMPANY

KGS®

KPMG

MorganFranklin®
CONSULTING

Guidehouse

tfc

WILLIAMS ADLEY

AGA®

www.agacgfm.org