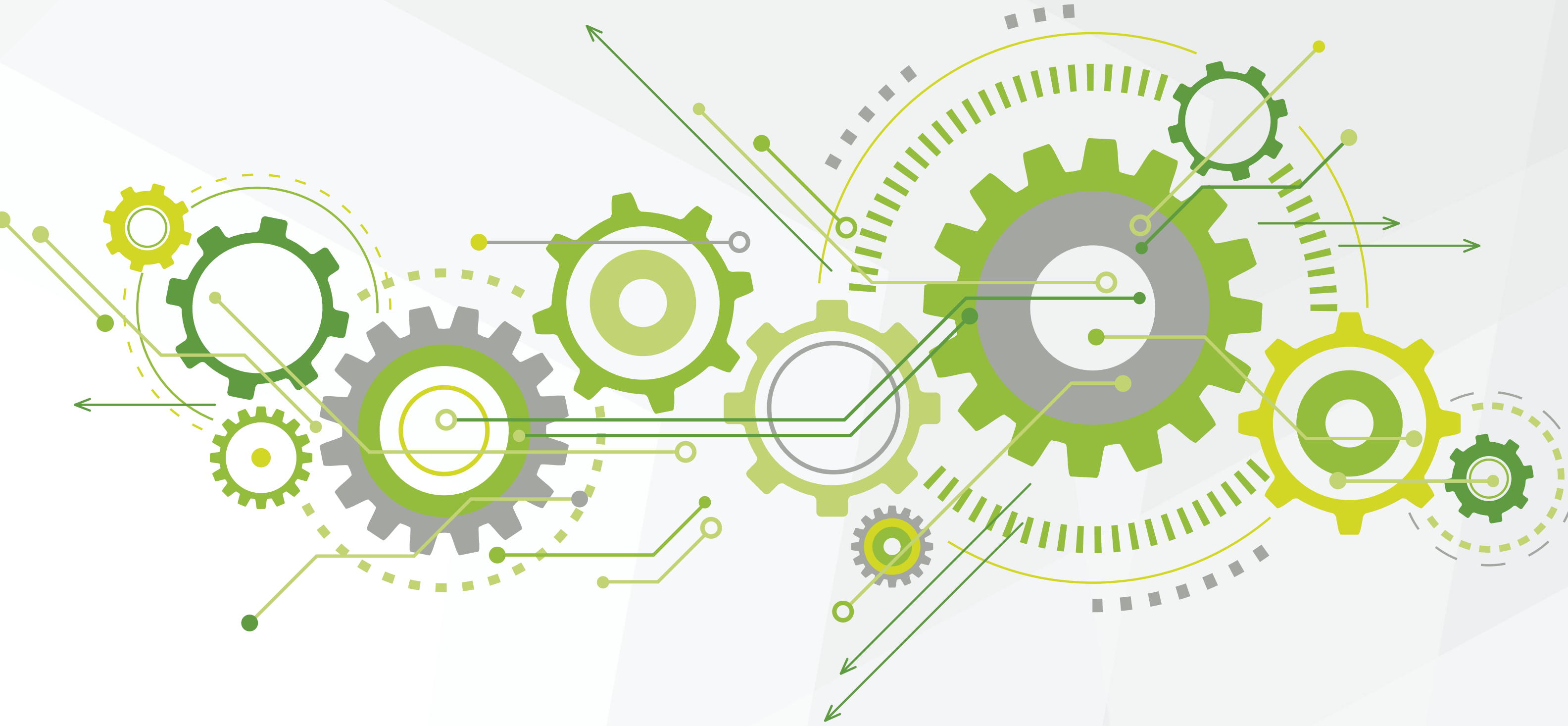


2020 ERM WORKSHOP

Leveraging ERM to Drive Organizational Value

June 12, 2020

AGA®

AFERM
Association for Federal
Enterprise Risk Management

ACKNOWLEDGEMENTS

AGA

Ann M. Ebberts, MS, PMP, Chief Executive Officer

Susan Fritzlen, Chief Operating Officer

Lyndsay McKeown, Senior Manager, Marketing & Design

Mary Margaret Yodzis, Editor

AFERM

Ken Fletcher, President

Varun Malhotra, Programs Committee Chair

In Appreciation

Special thanks to the Planning Committee who made the workshop possible and to all the sponsors for facilitating and capturing the roundtable discussions from which this report was produced. Additional thanks for the writing of this executive summary to the following contributors:

Sarah Choi, Guidehouse

Jambaar Stills, Guidehouse

Kerrigan Firth, Grant Thornton

Sam Twyman, Crowe

Donovan Chase, KPMG

AGA®

AGA is the member organization for financial professionals supporting 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
Association for Federal
Enterprise Risk Management

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 June 12, 2020, the Association of Government Accountants (AGA) and the Association for Federal Enterprise Risk Management (AFERM) held the fourth annual Enterprise Risk Management (ERM) Workshop with government professionals. Due to the COVID-19 pandemic, the 2020 workshop was a live virtual event for the first time. This workshop provided an opportunity for more than 200 professionals to learn the latest ERM thought leadership from senior government leaders and engage with government colleagues on ERM's impact on organizational value and performance.

The workshop focused on three areas:

1. Integrating Risk Management – Harnessing the Power of All Risk Disciplines
2. Implementing an Effective ERM Program – Perspectives of the Inspector General
3. Operationalizing the Risk Appetite Statement to Aid in Decision-making

Dan Kaneshiro, a senior policy analyst at the Office of Management and Budget (OMB), set the workshop's tone by asking attendees to view ERM beyond the lens of OMB Circular A-123 and Appendices A, B, and C. As ERM approaches its fourth year in the federal government, he said, OMB should stop "pushing" ERM guidance, and the federal ERM community should start "pulling" ERM forward. He also noted "pulling" in federal agencies is evident in expanding senior leadership roles sharing agency risks. The chief risk officer (CRO) no longer solely manages agency risks but collaborates with the agency's chief operating officer, chief financial officer, chief information officer, chief data officer, etc.

Kaneshiro said pulling is also apparent in forming the ERM Executive Steering Committee, an interagency group to promote and facilitate risk-aware culture in the federal government through an ERM framework and strategies. The collective ERM pull among federal agencies presents an opportunity to significantly advance ERM maturity for improved program mission accomplishment and contingency planning while driving risk-informed decision-making and resource prioritization.

The remaining structure of the workshop included presentations in each of the three focus areas listed above. In the first session, panelists included Larry Koskinen, CRO of the U.S. Department of Housing and Urban Development, Robert Milden, vice president for eGRC integrated solutions at Fannie Mae, and Col. Scott Ritzer, CRO of the Defense Logistics Agency. The panel discussed ways to integrate various risk disciplines in an organization to leverage collective strengths and coordinate efforts. They also identified strategies to address risks and challenges and integrate risk management functions within the entire organization.

In the second session, Temika Edwards, director of the policy, strategy, and risk division of the Office of Integrity and Quality Oversight at U.S. Department of Homeland Security Office of Inspector General (OIG); Theresa Perolini, director of the quality and integrity group at the U.S. Department of Education OIG; and Jessica Southwell, chief performance and risk management officer for the U.S. Department of Labor OIG, discussed the role of OIGs in promoting ERM in their agencies and OIG organizations. The panelists shared ERM implementation practices, insights from their oversight work on the integration of risk information, and perspectives on the value of ERM.

In the third session, Nahla Ivy, ERM officer at the National Institute of Standards and Technology (NIST); Jason Leecost, director of operational risk at the Government National Mortgage Association (Ginnie Mae); and Liz Ryan, managing director of ERM at Export-Import Bank of the U.S. (EXIM), discussed organizational risk appetite as a critical component of ERM program success. The panelists shared tips on developing an effective risk appetite statement and implementing it throughout an organization.

After the presentations, workshop attendees gathered in virtual small breakout groups for facilitated discussions with colleagues in the federal government. This report captures many of the ideas and real-life practices identified in these discussions to share with the broader government ERM community.

Session 1: Integrating Risk Management — Harnessing the Power of All Risk Disciplines

Sound ERM practices must be forward-looking, designed to help leaders make better decisions, identify threats, and raise awareness of previously unknown opportunities to improve government efficiency and effectiveness. ERM encourages horizontal and vertical communication channels to facilitate transparency and informed decision-making. It creates a structure for examining risks posed by likely events, assessing the probability of their occurrence, developing a risk-based approach to reduce the effects of events, preparing for immovable risks, and planning for recovery.

The shift to an enterprise (organizational) approach in risk management calls for change. Everyone at every level of an organization must know how and agree to identify, report, or elevate, manage, and mitigate risk. An entity must integrate ERM into each phase of operations and in every conversation for the capacity to see the event horizon. "Local" definitions of risk must be replaced by an enterprise risk lexicon to create a shared understanding of and language for risk. It means risk assessment (e.g., low, medium, or high risk) is more comprehensive. The entity calibrates the potential effects of an event one department deems "worth the risk" against the same risk elsewhere in the organization. Hence, it may not judge the risk worth it from an enterprise perspective. Organizations that successfully integrate various risk disciplines are ready and able to leverage collective strengths and coordinate efforts.

The group discussions for the first workshop session focused on identifying strategies to address risks and challenges to integrate risk management functions throughout the entire organization, specifically:

- Opportunities to leverage multiple channels of risk management to drive performance and improve outcomes.
- Critical governance considerations for an integrated risk management framework.
- Limitations and considerations associated with establishing an integrated ERM data strategy and management approach.

Opportunities to Drive Performance and Improve Outcomes

Participants reflected on the importance of integrating performance with ERM. At one agency, a single team handles these issues, and risk management is incorporated directly into strategic planning. A participant from another agency shared that a separate group is responsible for strategic planning; in this instance, the ERM team holds monthly meetings with strategic planning representatives to "insert ourselves into their processes in the hopes that the ERM program aligns to strategic goals." Participants collectively reflected on the importance of integration but noted the importance of understanding how to operationalize and integrate ERM in an organization.

Most participants noted their respective agencies are in the early stages of incorporating ERM with strategy but expressed confidence they were moving in the right direction. However, at two agencies with mature ERM programs, participants shared that ERM efforts focus on how risk management influences strategic initiatives. At one of these two agencies, ERM influence receives support from an established bidirectional or two-way communication pathway that uses strategic initiatives to shape the program. Additionally, agency leadership stays abreast of performance and controls to protect assets, which boosts teams' confidence in their risk mitigation.

Participants agreed that leveraging ERM in a purposeful way, in which they discuss risk and performance in tandem, empowers organizational decision-making as a keystone to culture, organizational transformation, and achieving strategic objectives.

Critical Governance Considerations for an Integrated Risk Management Framework

Successful ERM governance will fundamentally drive performance change; in turn, those performance changes will drive the success of an ERM program. This governance involves setting goals, tying organizational goals to department, team, and individual contributor goals, incorporating risk management in performance planning and annual performance review processes, and establishing key performance indicators (KPIs). It is critical to tie risk management to performance management. Additionally, participants noted several cultural elements which enhance or impede ERM governance, noting:

- **Location of ERM Leadership within an Organization** — Many participants shared that ERM functions are in various places within an organization. Some participants noted that CROs report to a CFO or secretary, and in other organizations ERM resides at a lower level within an office. Participants agreed that ERM programs often struggle to achieve buy-in if ERM's governance level is too low.

- **Levels of Stakeholder Engagement and Buy-in Involved with Governance** — One participant noted personalities as a driving force in ERM buy-in. For example, individuals who quickly recognize ERM's value will enhance and support governance, improve ERM success, and increase program fidelity. Whereas staff in more centralized components often do a good job socializing upwards in an organization, they often find it challenging to do so across an organization with different levels of resistance, i.e., report what is needed, but stay out of our business.
- **Being Consistent with ERM Methodologies, Standards and Establishing a Common Lexicon** — A participant shared that a single team owning ERM is most successful when ERM efforts and priorities are incorporated directly into strategic planning.
- **Communication on Governance Structure and Education on Risk Management** — Participants with mature ERM programs noted that governance structure, clear lines-of-sight to senior leadership, and education are keystones to success. Furthermore, an investment in educating the community across functions (i.e., program, financial management, IT) encourages cross-organizational collaboration and understanding. Participants noted that it is helpful to explain risks and context with multiple disciplines involved.

Limitations and Considerations with ERM Data Strategy and Management Approach

The most consequential characteristic of integrating ERM may not be that it is a "new" risk management approach but that it becomes an enterprise change initiative and decision-making tool. ERM enables connections where previous connections may have been weak or nonexistent. To do this, ERM leaders will want to find ways to standardize criteria, performance measures, and data to be more consistent throughout the organization. Sorting out irrelevant data while establishing a framework to transform data into meaningful information with a standardized form-fit-and-function enables more robust, strategically important data pulls for analysis and use in decision-making and planning.

Discussion leaders asked participants, "How is data playing a part in your current ERM conversations?" Responses were energetic and visionary. Some participants said they leverage ERM surveys and analyze data to evaluate risks, viewing data as a major driver in looking at ERM in general. Further, data can also communicate issues to leaders and other stakeholders.

Noting data as a mission-essential function, many participants added their sense of urgency in leveraging data in an ERM program. One participant shared this perspective: "Data is everything. A big component of what we do are these assessments of high-risk areas. We would not know what areas to dive into without the information from the components about what keeps them up at night. Everything the program does regarding risk and how to move forward is driven by data… Organizations must start with data planning, which is challenging. But it is difficult to standardize if there is junk in there. Data integrity is a struggle for the federal government in general."

Participants also shared current challenges and limitations with ERM and data today:

- "Our challenge is how to standardize, and which elements should be mandatory so that we can analyze the data."
- "How do you get buy-in from everyone, and how do you get the end-user to input the information you need?"
- "As a data person, one of the challenges from a people perspective is getting everyone on the same page about data integrity. Getting everyone to understand the importance of keeping master records and standardizing data definitions for a common understanding can be challenging."
- "Having access to various systems has been key. I have a data analytics person on my team. He keeps us ahead of the curve, and his access to data allows us to explore areas like information security, operations, etc. You must understand how systems work to understand how to extract appropriate data."

Session 2: Implementing an Effective ERM Program — Perspectives of the Inspector General

For the second session, the panel of OIG representatives shared their views on the promotion and implementation of ERM principles, under OMB Circular A-123, within the OIG community. They discussed the OIG's role in building an effective ERM program and leveraging the program to provide oversight. Throughout the discussion, they emphasized the need for management support to provide top-down endorsement and develop an effective communication plan with OIG leaders and staff. Describing the OIG's internal role in ERM implementation efforts, the panelists shared approaches taken to turn the concept of an ERM framework into an actionable, sustainable program and detailed the benefits of risk management in shaping and supporting agency operations. As detailed in **Figure 1**, building a successful ERM program requires continuous communication with all parties, and it begins by making the initial case.

Why Implement ERM?

According to *Quality Standards for Federal Offices of Inspector General*, published in 2012 by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), "The IG should provide for an assessment of the risks the OIG faces from both external and internal sources. Risk assessment includes identifying and analyzing relevant risks associated with achieving the OIG's objectives, such as those defined in strategic and annual performance plans and forming a basis for determining how risks should be managed." The key to making a case for an ERM program is to align risks with strategies to improve performance. The first step is to understand which risks affect the organization and then evaluate and prioritize them. By holding focused meetings or workshops with multi-disciplinary teams of experts, an organization can consider risk interdependencies and how they affect various departments. This engagement helps gain buy-in and facilitate communication, leading stakeholders to take ownership of risks and mitigation plans.

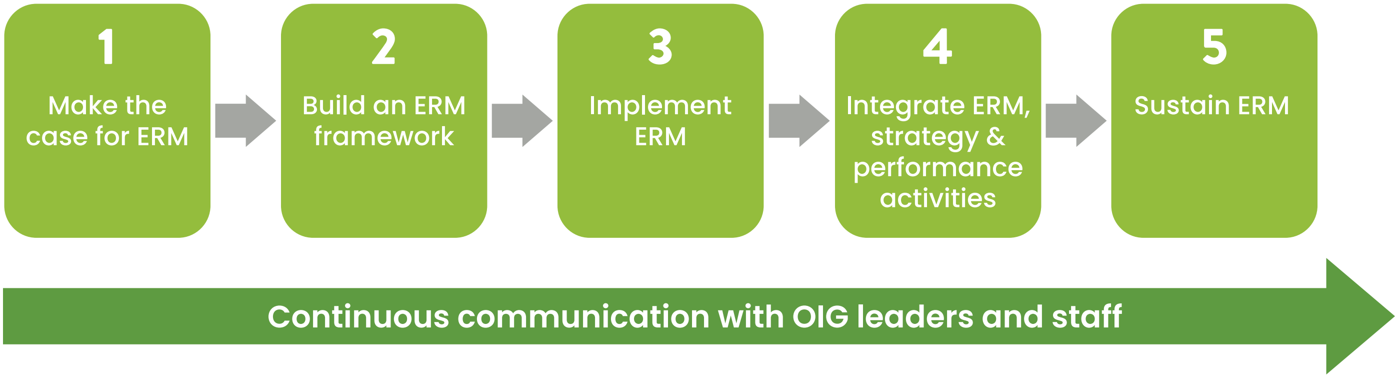
The panelists offered several essential points to help make a case for ERM:

- Ignored risks can become issues, which could lead to a crisis.
- Managed risks get quicker responses, use fewer resources, and offer more options; thus, they increase an organization's operating effectiveness.
- ERM improves the culture of the organization.
- OMB Circular A-123 requires ERM.

Using Risk Assessments to Build out a Risk Inventory

Once management and key stakeholders' support is secured, it is crucial to establish a formal risk-based plan. In this plan, the organization should identify and assess mission-critical risks in programs and processes that could affect operations. This evaluation produces a risk inventory to serve as the foundation for the ERM framework. Inputs for the risk register come from across the organization as well as external sources, as detailed in **Figure 2**. After creating the inventory, the organization constructs risk mitigation plans with input from its multi-disciplinary teams. One of the primary objectives of this plan is to align OIG resources to areas that deliver the most value to their respective agencies.

Figure 1: ERM Implementation



1 Make the case for ERM

2 Build an ERM framework

3 Implement ERM

4 Integrate ERM, strategy & performance activities

5 Sustain ERM

Continuous communication with OIG leaders and staff

Leveraging ERM in Oversight

The OIG plays an integral part in the development and implementation of an effective ERM program. When performing their oversight function, reliance on the ERM program guides the OIG in determining which areas of the organization hold the most risk and where their services will provide the most value in mitigating them. Through risk assessments of programs, evaluations of agency risk management, and audit and investigative work, the OIG helps identify and shape the agency risk inventory and provide feedback and recommendations to help the agency operate more efficiently and effectively. As the panel noted, communication lines between agency management and the OIG must be open to be effective. They need to agree on using ERM to improve agency programs and operations.

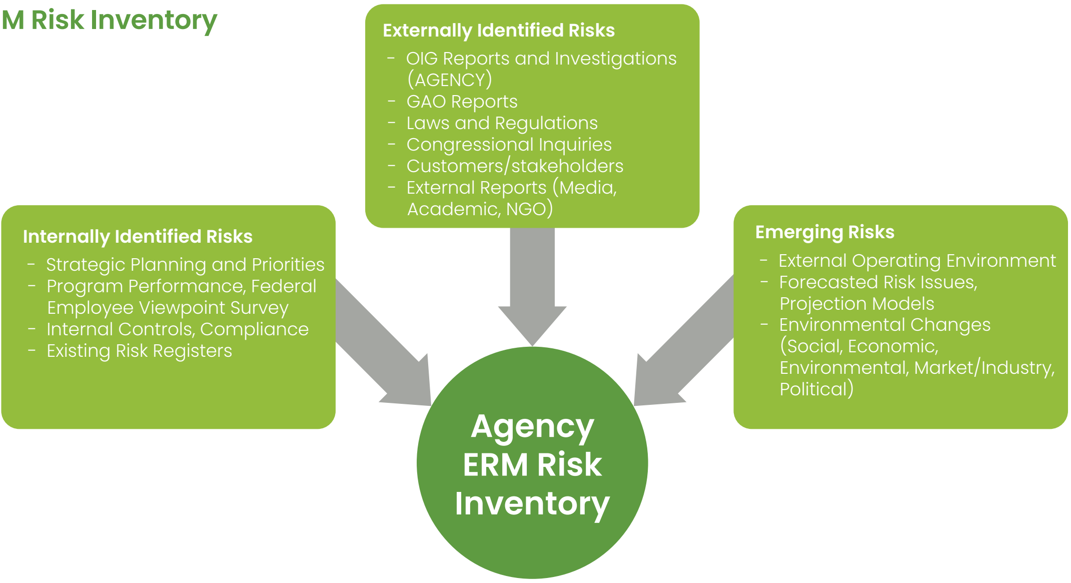
The OIG is not only a partner in helping to implement the ERM program; it also serves as the program evaluator through audits, evaluations, and investigations. The OIG determines risk factors and criteria through risk assessments, continuously fine-tuning the risk inventories, rating, and classifying agency risks, and utilizing the risk assessments to drive operational improvements. The agency can use the risk assessments, audits, and other evaluations to optimize performance by aligning the identified risks with strategic goals and objectives. Although some may not view an audit or investigation as a good thing for an organization, the testing of controls, identification of risks, and recommendations made to mitigate those risks all play an integral part in implementing and sustaining an effective ERM program.

Overarching Themes of Break Out Discussion

Implementing an ERM program produces its own set of challenges for each agency. In our post-session discussions, we noted some reoccurring themes voiced by participants, including:

- Please do not treat the risk program as a new concept. The goal should be to incorporate it into what already exists and link the risks back to people and processes.
- It is difficult to connect a risk assessment to A-123 requirements and communicate it in language everyone can understand.
- It is necessary to break down silos to communicate effectively and share information (e.g., create a common risk language, forums for discussion, etc.)
- It helps to make the program relatable to individual stakeholders and demonstrate the value of an ERM program. If positive outcomes are not compelling enough, illustrate potential adverse consequences of not implementing ERM.
- It is important to remember that every organization is different. A checklist and "one size fits all" approach does not necessarily work.
- Buy-in is crucial – buy-in from leadership, from the individual stakeholders, and from the OIG to further the program and prove its value.

Figure 2: ERM Risk Inventory



Externally Identified Risks
- OIG Reports and Investigations (AGENCY)
- GAO Reports
- Laws and Regulations
- Congressional Inquiries
- Customers/stakeholders
- External Reports (Media, Academic, NGO)

Internally Identified Risks
- Strategic Planning and Priorities
- Program Performance, Federal Employee Viewpoint Survey
- Internal Controls, Compliance
- Existing Risk Registers

Emerging Risks
- External Operating Environment
- Forecasted Risk Issues, Projection Models
- Environmental Changes (Social, Economic, Environmental, Market/Industry, Political)

Session 3: Operationalizing the Risk Appetite Statement of Aid in Decision-making

While OMB Circular A-123 states, “a formally documented risk appetite statement is not required,” it nonetheless emphasizes that risk appetite “is key to achieving effective ERM and is essential to consider in determining risk responses.” The third workshop session considered different ways to operationalize a risk appetite statement to aid in decision-making, and the breakout sessions continued to explore those thoughts. Many participants noted that their agencies do not currently have risk appetite statements and were looking for guidance on developing risk appetite statements and tolerances to apply in decision-making at all organizational levels. In most cases, agencies with relatively new or less mature ERM programs did not have risk appetite statements. They viewed the formal creation of risk appetite and tolerance as a step toward ERM maturity.

A key aspect of operationalizing risk appetite is understanding how to create the metrics on which risk appetite, and more specifically, risk tolerances, can be applied. Liz Ryan of EXIM described tailoring risk appetite within each of the top-level taxonomy areas of strategic, operational, financial, and legal risks. EXIM specifically operationalized risk appetite to examine risk scoring in each taxonomy, with heat maps constructed to establish where EXIM’s risk tolerance existed for each scored risk. They further refined results by individual risk metrics and set upper and lower limits, as needed.

Jason Leecost of Ginnie Mae explained his agency’s process to define high- and low-level metrics and tie them to the organization’s risk appetite and tolerance. After interviews with senior executives and directors, Ginnie Mae aligns risk appetite statements with individual management goals and objectives. Individual office-level business units set specific risk thresholds aligned with enterprise-level risk thresholds and tolerances. In this way, day-to-day risk tolerance follows management goals and objectives, which align with enterprise-level risk appetite tied to Ginnie Mae’s strategic objectives. A key consideration in making those linkages explicit was to show how each metric flowed from operational goals to strategic goals.

Similarly, in approaching risk appetite at NIST, Nahla Ivy began with a survey of senior leadership. She noted that aligning the perceptions of appropriate risk-taking with risk avoidance thresholds is a challenge for senior leaders. While leadership and line management should share thresholds, they tend to share only a desire to shape risk appetite. After identifying the misalignment, NIST worked to communicate with senior leaders about incorporating risk tolerance in their decision-making.

Workshop participants noted that surveys are typical for gathering information from leadership, management, and front-line staff to help formulate the individual risk tolerances aligned to risk appetite. However, many participants related challenges in translating risk appetite into a decision-making tool for their agencies. They cautioned against writing risk appetite statements that are merely mission statements. Some said composing the statements is only a simple “intellectual” or “paper” exercise because it lacks the value inherent in linking metrics and measurements.

Like the gap recognized at NIST, another gap derives from a common perception that agency leadership generally has zero risk tolerance for most to all business decisions. Participants recommended discussions with leadership about “accepting a tolerance of [some] risk and then managing it.” Participants identified tactics, including working through offsite retreats, to focus team discussions and bridge the gap. Focused meetings promote honest conversations about risks and build an appetite for strategic planning.

Unwillingness to embrace actual risk tolerance and vagueness in decision-support can cause the value of a risk appetite statement to deteriorate. Participants suggested multiple methods to avoid this situation, including:

- Sharing examples of well-written risk appetite statements and showing individual risk tolerances that were aligned.
- Working backward from previous management decisions in which risk revealed risk appetites and tolerances, even without the organization’s formal recognition.
- Considering the risk appetite framework made through past, unconscious risk decisions and modifying it for the present-day.
- Linking risk to budget decisions by showing visually, through heatmaps or sparklines, areas where risks breached established thresholds and using that information to decide on agency budgetary, procurement, and human resource allocations.
- Making extant risk tolerances actionable when explicitly linked to management and strategic goals.

Conclusion

As ERM is championed and matured across the federal government, agencies demonstrate a myriad of ways to integrate and leverage ERM for enhanced decision-making. This annual ERM workshop from AGA and AFERM affords a valuable opportunity for the federal ERM community to come together to share best practices and ideas with senior government leaders and colleagues. This year's ERM workshop allowed participants to gain valuable insights on integrating risk disciplines throughout an entire organization, consider ERM value, gather best practices from oversight entities for ERM implementation, and learn how to operationalize risk appetite statements.

Appendix: Participating Government Entities

Administrative Office of the United States Courts
Appalachian Regional Commission
Architect of the Capitol
Dormitory Authority of the State of New York
Equal Employment Opportunity Commission
Export-Import Bank of the United States
Federal Energy Regulatory Commission
Federal National Mortgage Association
Federal Reserve Board
Federal Retirement Thrift Investment Board
Federal Trade Commission
General Services Administration
Government Accountability Office
Library of Congress
National Aeronautics and Space Administration

- Office of the Inspector General

National Labor Relations Board
National Transportation Safety Board
New Zealand Inland Revenue
U.S. Office of Management and Budget
Pension Benefit Guaranty Corporation
Securities and Exchange Commission
Social Security Administration
U.S. Agency for International Development
U.S. Citizenship and Immigration Services
U.S. Department of Agriculture

- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service
- Office of Inspector General

U.S. Department of Commerce

- National Oceanic and Atmospheric Administration
- National Institute of Standards and Technology

U.S. Department of Defense

- Defense Health Agency
- Defense Logistics Agency
- Department of the Army
- Department of the Navy

U.S. Department of Education

- Office of Inspector General

U.S. Department of Health and Human Services

- Administration for Children and Families
- Health Resources and Services Administration

U.S. Department of Homeland Security

- Customs and Border Protection
- Cybersecurity and Infrastructure Security Agency
- Office of Inspector General

U.S. Department of Housing and Urban Development

- Government National Mortgage Association

U.S. Department of Justice

- Federal Bureau of Investigation
- Office of Inspector General

U.S. Department of Labor

- Office of Inspector General

U.S. Department of State

- Office of Inspector General

U.S. Department of the Interior
U.S. Department of the Treasury

- Bureau of Fiscal Service
- Internal Revenue Service

U.S. Department of Transportation

- Federal Aviation Administration

U.S. Department of Veterans Affairs

- Veterans Health Administration

U.S. Food and Drug Administration
U.S. House of Representatives
U.S. International Development Finance Corporation
U.S. Nuclear Regulatory Commission
U.S. Office of Personnel Management
U.S. Holocaust Memorial Museum
Washington Suburban Sanitary Commission Water

Thanks to Our Sponsors

AGA®

www.agacgfm.org

AFERM

Association for Federal
Enterprise Risk Management

www.aferm.org