

Thought Leadership for the Federal Enterprise Risk Management Community

Contents

The President's Corner.....	2
Sharing Your Success Stories.....	5
Thought Leadership	6
AFERM 20/20 ERM Vision Virtual Summit.....	14
ERM Events.....	17
AFERM's 2020 ERM Awards Winners.....	18
Thought Leadership	19
AFERM's ERM Podcasts	24
ERM News.....	26
AFERM's ERM Blog.....	28
AFERM's Communities of Interest/Practice	31
AFERM's 2020 Federal ERM Survey Results	32
AFERM Membership.....	35
Thought Leadership	36



Highlights

This 34th issue of the quarterly AFERM Newsletter includes thought leadership articles from ERM practitioners with EY, KPMG, Risk Pro Solutions, and the Bureau of the Fiscal Service. It also features the AFERM ERM Award winners of 2020 and AFERM's annual ERM Survey results for 2020.

Thought Leadership for the Federal Enterprise Risk Management Community

The President's Corner



AFERM President Ken Fletcher

Wrapping Up FY2020

By Ken Fletcher, AFERM President

The end of October marked the end of my tenure as AFERM President and I want to express my appreciation for that opportunity and honor. This past year has certainly been an unusual and often stressful as we learned to adapt to the health and economic consequences of the on-going pandemic.

Everything AFERM accomplishes is the direct result of the time and energy of a host of dedicated volunteers who give so generously of their time. Through their flexibility and resourcefulness, AFERM has continued to provide a range of offerings for our members. Please join me in extending our appreciation and thanks to our wonderful corporate sponsors, committee chairs, individual volunteers, and members of the Board for making that possible during this challenging time.

Key to the success of any ERM program is tone-at-the-top and the anticipated changes to agency political leadership could alter that tone regardless of who is elected President this year. According to the Partnership for Public Service – Center for Presidential Transition, for the last three Presidents about “43% of Cabinet secretaries, deputy secretaries and undersecretaries at 15 major agencies left their jobs” on average within 6-months of the President’s election to a second term

https://presidentialtransition.org/wp-content/uploads/sites/6/2019/11/Turnover-Report_11.7.19.pdf).

Should we elect a new President, the turnover of political leadership will be nearly 100%. The experiences and ERM program lessons learned from the pandemic provide a valuable perspective on how ERM can contribute to the success of these new political leaders. Doing so will help ensure continued support for ERM from the top of the agency.

Thought Leadership for the Federal Enterprise Risk Management Community

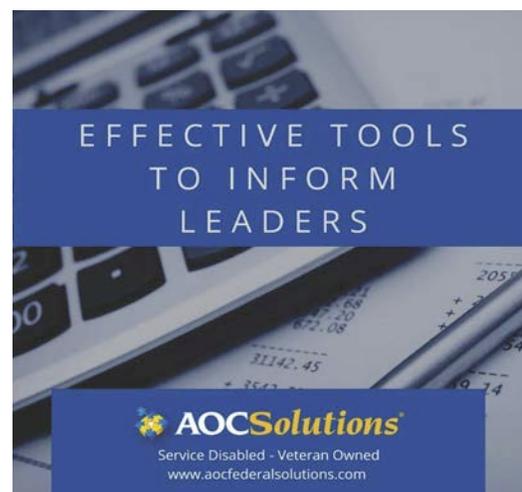
In closing, I want to congratulate our incoming President Nicole Puri, and welcome to our new President Elect Daniella Datskovska. We look forward to advancing AFERM and the federal government ERM profession under your leadership. Finally, I want to thank our out-going Board members - Past President Tom Brandt, and out-going Treasurer Fola Ojumu - for their service. Their leadership, dedication, and support to AFERM for the past 3 years has made AFERM a stronger organization providing a broader range of programs.

Thank you. Stay safe and stay healthy.

All the best,

Ken

Ken Fletcher, AFERM President, may be contacted at President@AFERM.org.



Thought Leadership for the Federal Enterprise Risk Management Community

Deloitte.



Designed for impact

At Deloitte, our people bring fresh perspective — from inside and outside government — to help you solve our nation's biggest challenges. From financial management and shared services to cyber, enterprise risk management, and anti-fraud, we drive bold and lasting results.

www.deloitte.com/us/federal-impact

Copyright © 2017 Deloitte Development LLC. All rights reserved.

Thought Leadership for the Federal Enterprise Risk Management Community

Sharing Your Success Stories

Communicating the value of ERM

Essential to the AFERM's Newsletter are success stories and thought leadership from ERM professionals. The concepts, innovations, and lessons learned shared by ERM professionals help advance the dialog and contribute to the maturation of the profession. We hope you found the contributions to this Newsletter as informative and thought provoking as we do! We kindly thank the following contributors to our latest Newsletter:

- **Ken Fletcher**, AFERM President, and President and founder of Kestrel Hawk Consulting
- **Chris Hare**, Senior Manager, **Valerie Lubrano**, Senior Manager, and **Baback Bazri**, Partner, EY
- **Donovan Chase**, Manager, Risk Consulting, and **Amanda Burke**, Manager, Risk Consulting, Federal Advisory, KPMG LLP
- **Soumya Chakraverty**, Managing Consultant, Risk Pro Solutions, and **Nicole Puri**, Chief Risk Officer, Bureau of the Fiscal Service

Please send your success stories or request for information on publishing a thought leadership piece to the AFERM Communications Committee at Communications@AFERM.org. The Committee is responsible for the AFERM Newsletter and is led by **Shelly Turner** with **Nadya Korobko**, both of Guidehouse, who may be contacted at sturner@guidedhouseFederal.com and nkorobko@guidedhouseFederal.com, respectively.

Crowe

**Smart decisions.
Lasting value.™**

crowe.com

Washington D.C. office

1455 Pennsylvania Ave NW, Suite 700
Washington, D.C. 20004

+1 202 779 9909

Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2019 Crowe LLP. CC2064-002A

Thought Leadership for the Federal Enterprise Risk Management Community

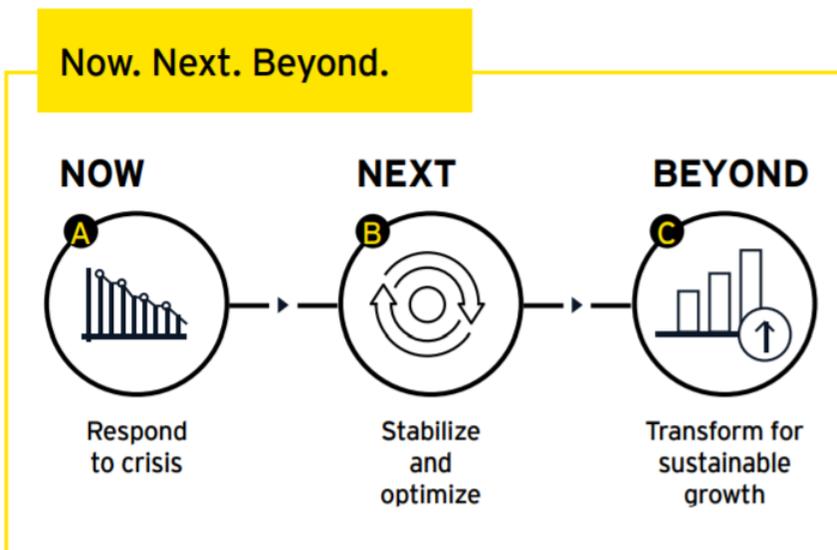
Thought Leadership

Enterprise risk management (ERM) in the COVID-19 world

By Chris Hare, Senior Manager, Valerie Lubrano, Senior Manager, and Baback Bazri, Partner, EY

Federal agencies are now faced with the prospect of quickly and effectively responding to the “new” business environment — there is a renewed focus on enterprise resiliency that relies on coordinated risk assessment, planning, monitoring and response across the enterprise. Regardless of whether a formally defined ERM program is in place, Federal agencies need to trigger coordinated, interdisciplinary teams to leverage risk activities to identify potential events that may affect the entity, manage risk within its risk appetite and provide reasonable assurance regarding the achievement of core mission objectives in support of the public.

To quickly address this new environment, agencies can prioritize vital actions by focusing on the steps that ERM and other risk functions can be taking: Respond to crisis, stabilize and optimize the business and transform for sustainable growth.



Thought Leadership for the Federal Enterprise Risk Management Community



While a majority of Federal agencies have been responding to COVID-19 since March, the virus continues to evolve and continues to present a challenge for the public as well as Federal agencies. During this phase, Federal agencies will be keenly focused on maintaining the safety and health of their people and citizens, rethinking the return-to-office paradigm, while still trying to manage to execute on mission essential functions. Key areas that ERM professionals should support include:

1. Enacting previously developed preparedness plans

- People engagement and safety — support continued business continuity by assisting with cross-functional response teams to provide for longer-term remote working arrangements or infection protections if remote working is not available and consider regular and transparent communications to inform and reassure employees
- Citizen engagement — keep citizens apprised of impacts, stay in contact with key stakeholders, review terms and conditions on commercial relationships and develop and test contingency scenarios for continuing operations in a restricted capacity
- Budget — support building a portfolio of budget improvement actions, assist in budget forecasting, tighten controls around citizen exposure and collections, and revisit budget allocations where possible
- Stakeholder engagement — understand critical stakeholder priorities, support scenario planning and analysis to reforecast, address emerging challenges with a crossfunctional team to establish decision governance and assist in coordinating and enabling clear communication

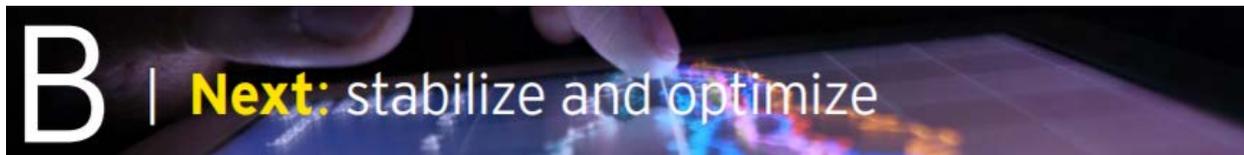
2. Conducting rapid impact assessments

Given the high fluidity of the external and internal environment, ERM professionals should initiate rapid risk assessments with leadership. While executing on preparedness plans, the priority of the risks to the organization will be changing quickly and leaders should be highlighting new risks that are surfacing. A weekly review of key risks to the organization, focused on the risks that need to be prioritized for response from limited resources, is key to managing the organization's risk profile and risk appetite in the time of crisis.

Thought Leadership for the Federal Enterprise Risk Management Community

3. Informing on risk mitigation gaps due to capital outflows

The efforts that Federal agencies put forth to manage their people, customers, stakeholders and their own financial stability require capital. Due to COVID-19, many Federal agencies are facing revenue shortages or budget cuts. ERM's role is to monitor risks where capital may be shifted away from existing risk mitigation and verifying that management is aware of new exposures that may surface as a result. For example, as many Federal agencies shift their workforce to a remote working model that puts additional stress on the IT infrastructure, they may require additional capital to mitigate the increased IT-related exposure. Given the necessity to focus on immediate organizational needs, having gaps in some risk mitigations may be acceptable to leadership. ERM professionals should assist leaders in identifying where gaps exist and help leadership make risk-informed decisions about capital allocation across their portfolio of risks.



Federal leaders need to consider that the definition of “business as usual” for their organization has likely changed. When the organization undergoes a significant disruption, it needs to reassess its performance objectives, strategy and risks to sustaining that strategy. With these changes in mind, refreshing the organization’s enterprise risk profile is essential. In order to do this, ERM professionals need to consider the following:

1. Determine if and how your organization’s performance objectives and strategies have changed

Every Federal organization measures performance, whether it’s qualitative or quantitative. The goals for performance may be quantitative — for example, decrease processing time for a government sponsored benefit by 10%, to more qualitative — such as to be one of the top employers in the local area. Given the changes that the world has seen with COVID-19, ERM professionals should consider asking questions such as:

- Do our performance goals still make sense or do they need to be adjusted? For example, is it realistic to decrease benefit processing time when our organization was disrupted for an extended period of time?
- Are our existing strategies positioning us to achieve the performance objectives?

Thought Leadership for the Federal Enterprise Risk Management Community

- Are we exposed to new outside risks that require us to re-evaluate our strategy?

Government executives may need to reassess and adjust their strategies in the post-COVID-19 world and reprioritize projects, as needed. If this does occur, ERM professionals should drive a refresh of the risk profile of the organization considering the updated performance objectives and/or strategies.

2. Consider the context of the new external environment

COVID-19 has shown us that the world is more connected than ever before. As stewards of risk within an organization, ERM professionals should affirm that economic and overall environment changes are considered as part of assessing the organization's risks.

Looking back on lessons learned from COVID-19 and identifying where the organization is vulnerable or interdependent is important. For example, while third parties may be diligently monitored with formal procedures, standardized contracts and other mitigations, the financial viability or operational integrity of third parties likely changed as a result of COVID-19. ERM professionals are implored to re-evaluate the risks.

3. Evaluate internal and operational changes

It is also important to account for changes to each organization and how those changes may impact the risk profile. Questions the ERM function should ask to help understand these changes may include:

- What is our strategy and how are we currently managing the disbursement of Coronavirus Aid, Relief, and Economic Security (CARES) Act funding and how will we manage future stimulus payments for my agency?
- Does our agency possess the in-house knowledge, capacity and enabling tools and technology to manage a large financial assistance program?
- How is our agency assessing the impact of financial assistance on citizens, businesses and other institutions?
- In disbursing CARES Act funds, how is our organization monitoring compliance; managing the risk of waste, fraud, abuse; and preventing de-obligations?
- Is there a significant increase or decrease in the demand for a particular product or service as a result of COVID-19? For example, increases in housing assistance program and unemployment insurance. Is it fair to assume that demand can come back to its previous levels?

Thought Leadership for the Federal Enterprise Risk Management Community

Did we furlough people and are now operating with fewer resources? Related to these questions, the acceptable risk tolerance levels will need to be revisited. Similar to Step 3 “Respond to crisis” above, allocating budget singularly to the COVID-19 pandemic response may have pulled budget from other important risk mitigation efforts and the organization may now be operating outside of previously defined acceptable risk tolerances. For example, an organization with five key cyber risks may now have a reduced workforce and may not be able to address patching or mitigation on system configuration or cyber awareness around potential phishing attacks. Keeping this in mind, the individual risk tolerances and overall performance risk appetite will need to be revisited and potentially adjusted.

4. Don't forget the upside of risk

While COVID-19 has resulted in negative impacts across multiple industries, it is important to consider potential upside opportunities. ERM professionals can help their agency identify where there may be a desire to take on more risk. In the Federal space, ERM can help executives and other business leaders identify new opportunities for growth. For example, some agencies may be able to recognize significant costs savings related to employee travel that could be repurposed to shore up technology needs given the shift to a virtual workplace during the pandemic. Additionally, Federal agencies can reconsider their commercial real estate leases and determine opportunities to lessen their real estate footprint and repurpose funds accordingly.

Being agile is important to capture new opportunities. Federal agencies need to consider how they can adapt their operations or services to align with the revised needs of citizens. The role of the ERM professional should be focused on determining that the risks and/or opportunities are assessed to align with the organization's adjusted risk tolerance levels. In the same example as above, understanding the risks associated with repurposing employee travel budgets should be a key part of the analysis prior to making a final decision.

Reassessing risks or new opportunities does not need to be cumbersome and time-consuming. Keeping the assessment simple and utilizing technology and automation will speed the process. Reassessing the risk profile will provide vital information to help leaders make risk-informed budget allocation decisions to stabilize and optimize operations as recovery and rebuilding happens.

Thought Leadership for the Federal Enterprise Risk Management Community



The final step is to look beyond COVID-19 and position ERM to add organizational value for 2020 and beyond. Federal leaders and agency executives will likely be asking what can be done to be better prepared for risks in the future and it will fall on ERM professionals to improve on the existing risk process. Potential areas of focus may include:

1. Transforming from qualitative to quantitative (quantifying risk exposures)

Recent events have shown the value of quantifying risk when we were presented with the “flatten the curve” distribution of COVID-19 cases. Understanding the quantitative exposure of a risk and comparing it to the acceptable risk tolerance levels will play an instrumental role in informing leaders’ resource allocation decisions. The change in the overall economic and business environment implores revising the underlying scenarios that are the base of the quantification and providing an updated value of risk exposure to the agency. A practical way for an agency to increase their overall program maturity is to pilot risk quantification with one to three key risks. The pilot will provide leadership with objective risk insights and allow leadership to determine the value of expanding risk quantification to the rest of the risk portfolio.

2. Leveraging data analytics and metrics to support ongoing risk monitoring

Once risk exposure and tolerances are better understood, risk monitoring should be part of the ongoing activities of the ERM function. Agencies must develop key risk indicators (KRIs) to support actionable risk monitoring to provide some early warnings of possible risk changes. Each risk must have unique KRIs and ERM professionals can assist business leaders in identifying and tracking the appropriate metrics.

In summary, ERM plays an instrumental role in helping Federal agencies achieve their strategic goals and performance objectives. COVID-19 is an example of an external risk event that drastically impacted operations for many agencies. But with the right approach, ERM will play a critical role in responding, stabilizing and optimizing, as well as transforming agencies for sustainable growth.

Thought Leadership for the Federal Enterprise Risk Management Community

Chris Hare may be reached at chris.hare@ey.com, **Valerie Lubrano** may be reached at valerie.a.lubrano@ey.com, and **Baback Bazri** may be reached at baback.bazri@ey.com.



About EY

EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2020 Ernst & Young LLP. All Rights Reserved.

US SCORE no. 10315-201US

CSG No. 2008-3544662

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM 20/20 ERM Vision Virtual Summit

Thank you to AFERM Summit 2020 speakers and moderators!



We hope you were among the more than 400 ERM professionals in attendance. This year's Summit Planning Committee is led by **Meredith Stein** of the National Institutes of Health and **Marianne Roth** of the Consumer Fraud Prevention Bureau. Below is their sincere thank you to all of the speakers and moderators to help make this year's Summit a success.

Dear Summit Speakers and Moderators,

AFERM would like to extend our sincere thanks for making the time to speak and moderate the breakout sessions for the 13th Annual AFERM Summit. This was the first year that the Summit was 100% virtual. We appreciated your flexibility and patience as we transitioned to this new and exciting format, especially under difficult circumstances. You made a lasting impression on the Summit participants.

We acknowledge all our session speakers and moderators for their unique contributions (in alphabetical order):

1. Vivek Arora, Head, Office of Risk Management, International Monetary Fund
2. Merline Barrington, Lead, ERM, New York New Jersey Port Authority
3. Gabriel Benincasa, CRO, Securities and Exchange Commission
4. Thomas Brandt, CRO, Internal Revenue Service
5. Atisha Burks, Senior Accounting and Finance Leader, Department of Navy
6. Donovan Chase, Advisory Manager, KPMG
7. Tom Easthope, Director, ERM, Microsoft
8. Adrian Evans-Burke, Lead Risk Analyst, Library of Congress
9. Preston Finley, Director, Foresight, Strategic Planning and Risk Management, Department of Veterans Affairs

Thought Leadership for the Federal Enterprise Risk Management Community

10. Mike Frueh, Deputy Assistant Secretary, Office of Enterprise Integration, Department of Veterans Affairs
11. Alyssa Fusisi, Principal, Kearney & Company
12. Chris Hare, Senior Manager, Ernst & Young
13. Thomas Holland, Director, Guidehouse
14. Bernard Jenkins, Director of Business Operations, Department of Health and Human Services, Office of the Assistant Secretary for Financial Resources
15. Larry Koskinen, CRO, Department of Housing and Urban Development
16. Kate Kraycirik, Director, Enterprise Risk Management, MD Anderson
17. Jill Lennox, ERM Team Lead, Federal Deposit Insurance Corporation
18. Bonita Mannings, Personnel Psychologist, Center for Veterinary Medicine, Office of Management, Food and Drug Administration
19. Alice Miller, CRO, U.S. International Development Finance Corporation
20. Patrick Murphy, Commissioner of the New York State Division of Homeland Security and Emergency Services
21. Dr. James Nelson, Chief Diversity Officer, Office of Minority Health and Health Equity, Centers for Disease Control and Prevention
22. Bobbi-Jo Pankaj, Managing Director, Grant Thornton
23. Stephen Quinn, Senior Computer Scientist, Information Technology Laboratory, National Institute of Standards and Technology
24. Mick Reed, Senior Director, Strategy and ERM, VF Corporation
25. John Skober, Branch Head, Financial Improvement and Audit Readiness, Department of Navy
26. Alyssa Smiley, Acting Director, Risk Management and Assurance, Department of Homeland Security
27. Kate Sylvis, Director, Guidehouse
28. William Tillman, Senior Agency Information Security Risk Officer, National Credit Union Administration
29. Marshall Toburen, Risk Management Strategist, RSA
30. Sean Vineyard, 11th Hour Service
31. Cynthia Vitters, Managing Director, Deloitte

Thought Leadership for the Federal Enterprise Risk Management Community

We appreciate your continuous support in furthering enterprise risk management across the AFERM Community.

Thank you,
AFERM

You may contact the **Summit Planning Committee** at Summit@AFERM.org if you have suggestions and the **Volunteers Committee** at Volunteers@AFERM.org if you're interested in volunteering with AFERM.



IRIS
INTELLIGENCE

*Intuitive web based software & solutions
developed for Federal & Local Government*

MANAGING TOMORROW ...TODAY

<u>Products & Services:</u>	<u>Software Features:</u>
➤ Enterprise Risk Management	✓ Risk Identification Triggers
➤ Project, Program & Portfolio Risk Management	✓ Qualitative & Quantitative Risk Assessment
➤ Information Risk Management & Cyber Security	✓ Out of the Box & Custom Report Templates
➤ Internal Controls & Compliance	✓ Automated Email Reminders & Secure Audit Trail
➤ Issue Management	✓ Microsoft Office and Schedule (IMS) Integration
➤ Systematic Innovation & Opportunity Management	✓ Quickly embed principles from ISO 31000, PMBoK, OMB A-123, NIST SP 800-37, NIST SP 800-53, ISO 27000 family & many more
	✓ Quick and easy installation & configuration

info@irisintelligence.com | www.irisintelligence.com | Phone: (646) 461-7475

Thought Leadership for the Federal Enterprise Risk Management Community

ERM Events

Upcoming events of interest to ERM practitioners

Following is a list of events upcoming that may be of interest to ERM practitioners.

Event (Click Name for Link to Event Information and Registration)	Organization	Date	Location
SimErgy: December ERM Boot Camp <i>Note: 20% discount for AFERM members</i>	SimErgy	December 8-9	Virtual

Please visit our website for more information at <https://www.aferm.org/events-list/>.

Varun Malhotra of Guidehouse coordinates the AFERM programs. He may be contacted at Programs@AFERM.org.

MILCORP PEOPLE MAKING THE DIFFERENCE | WWW.MILCORP.COM

40 YEARS OF PROVIDING
FINANCIAL SERVICES TO THE FEDERAL GOVERNMENT

SMART, PROACTIVE & PERSONALIZED SOLUTIONS

- >> Financial, operational & cyber risk identification
- >> Risk management software integration supporting risk tracking, controls & mitigation

ACCOUNTING | FINANCIAL SYSTEMS | BUDGET & RECONCILIATIONS
ENTERPRISE RISK MANAGEMENT | RISK MANAGEMENT SYSTEMS

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM's 2020 ERM Awards Winners

Congratulations to this years winners!

At the 2020 AFERM ERM Summit Training on September 10th, the 6th annual ERM Awards were announced for leaders recognizing their contributions to AFERM and in advancing ERM in the Federal Government. This year's winners include the following:

ERM Leaders of the Year

- Marianne Roth, Consumer Fraud Protection Bureau
- Curtis McNeil, Architect of the Capitol

ERM Professional of the Year

- Andy Tiedman, U.S. Department of Agriculture

AFERM Volunteers of the Year

- Edward Hau, ASR Analytics
- Meredith Stein, National Institutes of Health

AFERM's "ERM Leader of the Year" award honors leaders in the Federal sector that have demonstrated outstanding and sustained leadership, while making exceptional contributions to advancing the ERM discipline within the Federal sector. This award is available to current Federal sector employees.

AFERM's "ERM Professional of the Year" award honors Federal professionals who have demonstrated exceptional initiative, professional development, achievement, and leadership potential early in their career. This award is available to current Federal sector employees.

AFERM's "ERM Hall of Fame" award honors professionals who made extraordinary contributions to advancing the ERM discipline within the Federal sector. This award is available to current and former Federal sector employees.

AFERM's "ERM Volunteer of the Year" award honors professionals committed to the advancement of ERM within the Federal Government through their service to AFERM, a 100% volunteer-run organization. Providing their time and effort allows AFERM and its members to achieve all that we do and benefits the ERM community with their shared knowledge and skills. This award is available to all AFERM members/volunteers.

For more on AFERM's ERM awards, please visit our site at <https://www.aferm.org/awards/>.

Thought Leadership for the Federal Enterprise Risk Management Community

Thought Leadership

Practical Considerations for Risk Appetite Development with Risk Governance

By Donovan M. Chase, Manager, Risk Consulting, and Amanda Burke, Manager, Risk Consulting, Federal Advisory, KPMG LLP

A challenge for many agencies is how to link departmental-level strategic risk concerns with tactical and operational activities. Commonly, organizations establish ERM programs to manage risk at a department level with an overall strategic view, while working with existing front-line managers who approach risk with more concern for day-to-day activities. This challenge of uniting an agency's strategic vision with the evaluation of operational level risks is frequently addressed through the use of Risk Appetite and Tolerance. Defining risk tolerance at the strategic level enables agencies to align the operational level risk management with the strategic vision articulated by agency leadership.

The need for risk appetite and tolerance is noted in Office of Management and Budget (OMB) Circular A123 directly: "The concept of 'risk appetite' is key to achieving effective ERM, and is essential to consider in determining risk responses. Although a formally documented risk appetite statement is not required, agencies must have a solid understanding of their risk appetite and tolerance levels in order to create a comprehensive enterprise-level risk profile."¹

Who has the authority to establish risk appetite and tolerance? The natural answer is whatever risk governance authority exists for an agency. "Agency governance should include a process for considering risk appetite and tolerance levels."² The nature of that governance is also defined, "[S]enior management develop and implement core policies and procedures with respect to enterprise risk management, including developing a process to define risk appetite, and establish risk thresholds accordingly."³ Furthermore,

This challenge for Federal agencies is establishing the process by which risk appetite and tolerance can be successfully created, and thereby align their day-today tactical risk decisions against the agency's strategic direction.

¹Office of Management and Budget. (2016). *OMB Circular No. A-123. Management's Responsibility for Enterprise Risk Management and Internal Control*. [Washington, DC]: Executive Office of the President, p. 13. Retrieved April 28, 2019, from <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf>

²(Office of Management and Budget, 2016) p.13

³(Office of Management and Budget, 2016) p.12

Thought Leadership for the Federal Enterprise Risk Management Community

NIST Special Publication 800-39 *Managing Information Security Risk*, notes the need for organizational risk governance (March 2011), “Senior leaders/executives establish the risk tolerance for organizations both formally (e.g., through publication of strategy and guidance documents) and informally (e.g., through actions that get rewarded and penalized, the degree of consistency in actions, and the degree of accountability enforced)”⁴ (NIST 800-39, p.29). Creation of an agency’s risk tolerance(s) is inherently a directional exercise which must originate from governance and flow throughout the agency to establish the framework for risk decisions.

As a practical matter, ERM professionals often desire to utilize existing operational structures within an agency to develop the overall agency program. As a good general business practice, managers will implement risk assessment, risk monitoring, and risk response techniques without the initiation of a formal agency-wide ERM implementation, and it is natural to want to take advantage of the efficiency that using pre-existent processes offer. Such an approach offers cost savings because it leverages these effective, pre-existing methods that meet operational needs. Management is also comfortable knowing that their pre-existing approach to risk management does not need to change.

These are real advantages to using federated approaches to risk assessment, monitoring, and management within an agency, but such federated approaches also can present obstacles to aligning operational concerns with strategic vision. Since these front line risk assessment processes were built to address specific day-to-day risk concerns of management, they are not inherently aligned to respond to the view of risk at the strategic level, and may not address the same risk indicators or risk reporting needs of agency leadership. Individual approaches to risk tolerance likewise are frequently designed to address specific operational concerns and individual office or division priorities.

In order to successfully bridge strategic agency goals with operational concerns, the entity must determine the approach to articulating risk appetite and governance and cascade that approach down and through the organization. This top level set of guidance and limits on risk provide the foundation and bounds by which the agencies’ risk programs and managers can operate. Such explicit guidance can be contained in a Risk Management Council charter, for instance stating that the Council “will document agency-wide guidance for risk appetite and tolerance” as one of its activities. Alternatively, it is even possible that this responsibility could be delegated to a Chief

⁴National Institutes of Standards and Technology Join Task Force Transformation Initiative (NIST) (2011). *NIST Special Publication 800-39 Managing Information Security Risk: Organization, Mission, and Information System View*, p.29. Retrieved June 25, 2020, from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>

Thought Leadership for the Federal Enterprise Risk Management Community

Operations Officer (COO) or Chief Risk Officer (CRO). Irrespective of the method chosen, there must be a governing authority that can develop and implement an agency's risk appetite and tolerance.

This authority does not need to supersede specific thresholds that may vary internally at the agency, however. An agency's risk appetite sets the baseline for appetite and tolerance, but individual offices, divisions, and programs may set more stringent standards for establishing tolerances and/or breach limits based on the nature of the risk. Individual office, division, or program level tolerances can help inform agency leadership of the practical limits of risk tolerance that have already been deployed, using measurable data that is already available.

Risk governance at the agency level also provides the structure for risk monitoring and executive reporting throughout the organization. By using an agency-wide risk structure, operational risk managers and leadership begin discussing risk and tolerances in the same language. This brings more transparency to risk decisions. Any metrics the agency wishes to establish to oversee and monitor the ERM program should be based on these foundational risk tolerances, and individual offices should use them as a starting point in modeling their approach. For instance, consider an agency that has embraced a strategic risk appetite of "[t]he agency will accept a moderate risk of default in pursuit of providing loans to businesses in support of the agencies mission." In accordance with this risk appetite, the agency determines an acceptable default rate of 7% for a given loan program.

However, it would be reasonable for program administrators to determine that, for an individual cohort within that loan program, a default rate of 5% is tolerable, so as to maintain a default rate aligned with the entirety of the program. This 5% tolerance would be acceptable to the agency as whole, though more narrow than what was specified. Conversely, it is unlikely that establishing a cohort default tolerance of 12% would be appropriate, unless the program could demonstrate that this 12% rate for the individual cohort would not bring the overall program outside of the 7% agency limit and that the 12% limit was adopted in order to specifically achieve other mission goals.

Ultimately, without centralized, authoritative risk governance at the agency level and a subsequent risk appetite and tolerance based on agency goals and objectives, the ability to have an ERM program that properly examines risk reporting within the appropriate strategic framework is imperiled. By defining the risk governance structure and the method by which an agency will express its risk appetite and tolerance early on in the ERM implementation process, the agency better ensures positive outcomes overall. And, widely communicating and enforcing the appetite and tolerance levels helps inform and align these elements throughout even the most distributed agencies.

Thought Leadership for the Federal Enterprise Risk Management Community

Donovan Chase may be reached at donovanchase@KPMG.com and **Amanda Burke** may be reached at aburke@KPMG.com.

This article represents the views of the authors only, and not necessarily the views or professional advice of KPMP LLP. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.



The advertisement features a dark blue background with a network of glowing blue nodes and lines. A central graphic shows a yellow radar screen with a red crosshair and the words "Risk Radar" in a bold, yellow, sans-serif font. Below this, the text "Risk Radar® Enterprise" is written in yellow, followed by "a customizable Risk Management Solution with comprehensive RISK, ISSUE and OPPORTUNITY reporting." in a smaller yellow font. At the bottom left is the "PRO-CONCEPTS" logo in white. To the right, contact information is listed: "CALL (757) 637-0440", "Email: RiskRadar@ProConceptsllc.com", and "www.ProConceptsllc.com". At the very bottom, there are three social media icons: Facebook (@RiskRegister), LinkedIn (@proconceptsllc), and Twitter (@RiskRadar).

Thought Leadership for the Federal Enterprise Risk Management Community

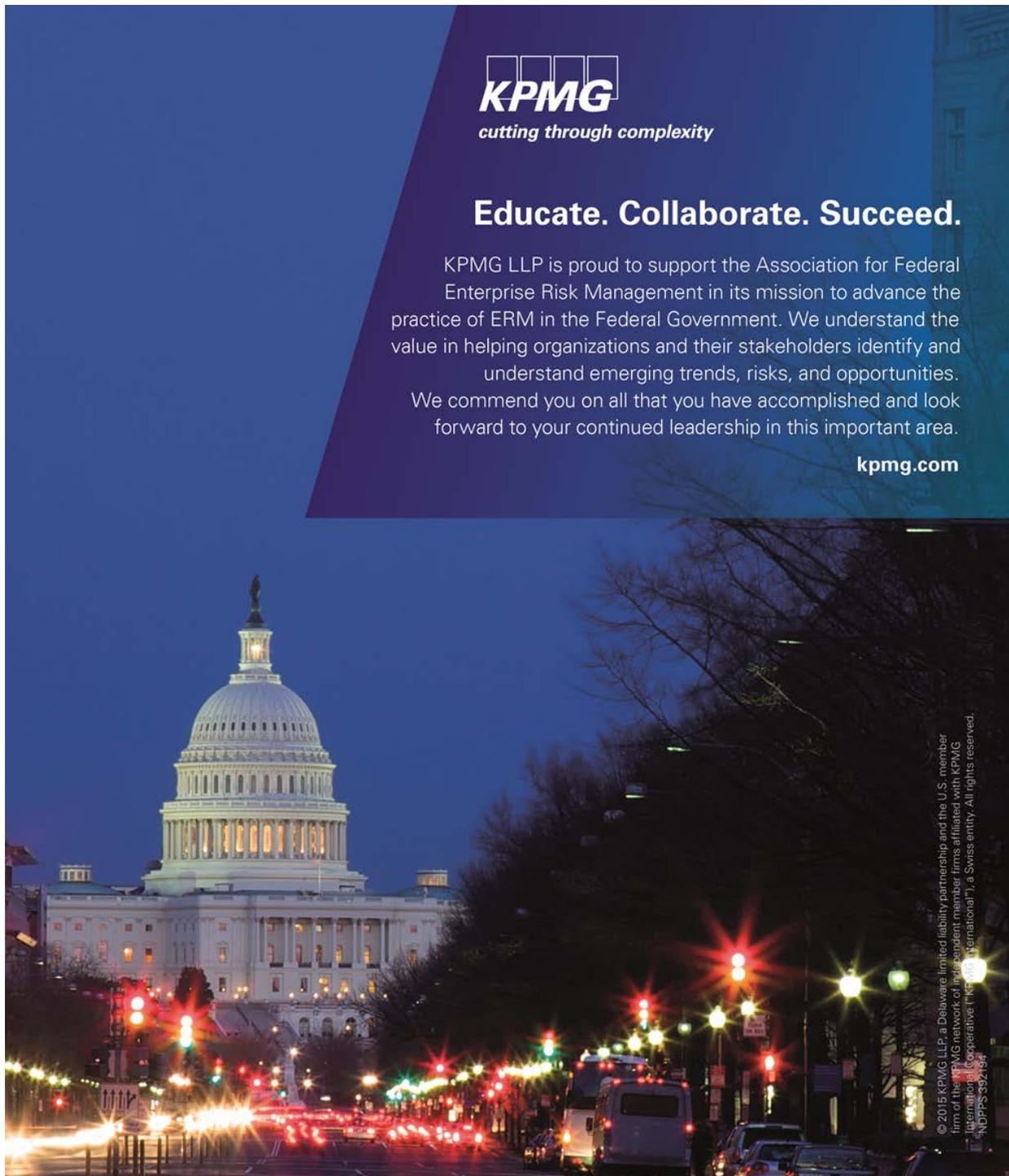


cutting through complexity

Educate. Collaborate. Succeed.

KPMG LLP is proud to support the Association for Federal Enterprise Risk Management in its mission to advance the practice of ERM in the Federal Government. We understand the value in helping organizations and their stakeholders identify and understand emerging trends, risks, and opportunities. We commend you on all that you have accomplished and look forward to your continued leadership in this important area.

kpmg.com



© 2015 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 392.194

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM's ERM Podcasts

AFERM's podcasts continue the ERM dialogue

Be sure to check out the 38 Risk Chat podcasts on our website featuring ERM subject matter relevant to the Federal sector. If you are interested in participating on a podcast, please contact Paul Marshall, MILCorp, and Tal Seaman, Navigator Solutions.

The podcasts are accessible on AFERM's website at <https://www.aferm.org/aferm-risk-chats/>. The podcasts are listed below with active links.

- Episode 1: ERM at the Internal Revenue Service
- Episode 2: ERM at Housing and Urban Development (HUD), Public and Indian Housing
- Episode 3: RIMS-CRMP-FED Micro-credential
- Episode 4: ERM at the U.S. Coast Guard
- Episode 5: ERM at Pension Benefit Guaranty Corporation
- Episode 6: ERM at the National Institutes of Health
- Episode 7: ERM at U.S. Department of Agriculture, Rural Development
- Episode 8: ERM at Corporation for National and Community Service
- Episode 9: ERM at Ginnie Mae
- Episode 10: ERM at King County
- Episode 11: GAO's High-risk List
- Episode 12: ERM at the HUD Office of the Inspector General (OIG)
- Episode 13: ERM Book – Beyond the Basics
- Episode 14: ERM at the U.S. Department of Veterans Affairs
- Episode 15: ERM at the National Aeronautics and Space Administration
- Episode 16: Cybersecurity and ERM at Mecklenburg County
- Episode 17: Data Analytics for ERM
- Episode 18: ERM at HUD
- Episode 19: Risk Appetite at U.S. Agency for International Development (USAID)
- Episode 20: National Risk Management
- Episode 21: AFERM Small Agency Community of Practice

Thought Leadership for the Federal Enterprise Risk Management Community

- Episode 22: AFERM Cybersecurity Community of Interest
- Episode 23: ERM at the U.S. Food and Drug Administration
- Episode 24: Strategic Risk
- Episode 25: 10 Years of ERM
- Episode 26: The Costs and Benefits of ERM
- Episode 27: AFERM Data Analytics Community of Practice
- Episode 28: National Institute of Standards and Technology Cyber Security
- Episode 29: ERM at the U.S. Department of Justice, Office of Justice Programs
- Episode 30: Pension Benefit Guaranty Corporation OIG
- Episode 31: ERM at the Canada Revenue Agency
- Episode 32: ERM at the OCC
- Episode 33: AGA AFERM ERM Workshop Lessons Learned
- Episode 34: Our Favorite Podcasts
- Episode 35: Value-based Management
- Episode 36: AFERM President Ken Fletcher
- Episode 37: Operationalizing USAID's Risk Appetite Statement
- Episode 38: ERM Around the World

Paul Marshall may be contacted at pmarshall@milcorp.com, and **Tal Seaman** may be contacted at tseaman@navigatorso.com.

Thought Leadership for the Federal Enterprise Risk Management Community

ERM News

Staying current on ERM news with AFERM's Newsfeed

Following are headlines of just some of the many news articles identified by AFERM as relevant to Federal ERM this past quarter on our ERM News page with active links:

- Building Strong Risk Committee Relationships
- Return-to-work Lessons from Major League Baseball
- Cybersecurity Policies for Remote Work
- Frameworks for Data Privacy Compliance
- Disaster Assistance: FEMA Should Take Additional Actions to Strengthen Fraud Risk Management for Public Assistance Emergency Work Grants, Sep 29, 2020
- OIG Special Report - FY 2019 Purchase Card Risk Assessment
- How Risk Professionals can Enable Digital Transformation
- Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy, Sep 22, 2020
- Critical Infrastructure Protection: Treasury Needs To Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts, Sep 17, 2020
- 10 Ways New Digital Platforms can Help Manage Multinational Risk
- Telecommunications: FCC Should Take Action to Better Manage Persistent Fraud Risks in the Schools and Libraries Program, Sep 16, 2020
- How Leaders can Balance Working from Home and Returning to Work
- COVID-19 Litigation and the Nursing Home Industry
- Compliance Expectations Amid the COVID-19 Crisis
- Preventing Insider Threats to Cybersecurity
- Time and Attendance: Agencies Generally Compiled Data on Misconduct, and Reported Using Various Internal Controls for Monitoring, Aug 31, 2020
- 7 Tips for High-risk Organizations Reopening During COVID-19
- Customer-Driven Risk Management
- Challenge Grant Competition: Re-Thinking Government Management and Operations Given The Impact Of COVID-19
- Litigation Risks of Videoconferencing Tools

Thought Leadership for the Federal Enterprise Risk Management Community

- 4 Ways to Build Influence as a Risk Manager
- Crisis Plans Minimize Cyberattack Disruption
- FCPA Risk in the Health Care Sector
- Cybersecurity Risk Management – Resources for Agency Action
- How Chief Risk Officers Can Add Value in a Crisis
- Spending Risks Shift as the Pandemic Continues
- The Link Between ERM and Organizational Financial Performance
- Preventing Paycheck Protection Program Loan Scams

To view the AFERM Newsfeed, visit “Resources” on the AFERM website and choose “Newsfeed” or use the following link: <https://www.aferm.org/erm-newsfeed/>.

Your feedback and suggestions on the AFERM Newsfeed is welcome and may be submitted at AFERM.Webmaster@gmail.com.

tfc | CELEBRATING 15 YEARS OF EXCELLENCE | Every move is strategic.

PERFORMANCE
OUTCOMES

**ASK US HOW WE CAN HELP YOU
IMPROVE YOUR PERFORMANCE**

We Listen | We Innovate | We Deliver

240.453.6288 | ddatskovska@tfeci.net | tfeci.net

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM's ERM Blog

ERM resources for Federal practitioners

AFERM's "Ask the Experts" blog continues to generate some great conversations on ERM! Our blog is hosted by ERM professionals **Tom Erickson**, NTT Data, **Ken Fletcher**, Kestrel Hawk Consulting, and **Sean Vineyard**, 11th Hour Consulting.

Here are some recent discussion topics with active links:

- Is ERM just a more mature way to implement internal controls (part 1 of 2)?
- Is ERM just a more mature way to implement internal controls (part 2 of 2)?
- Office, bureau or agency-wide ERM implementation. Which is best (part 1 Of 2)?
- Office, bureau or agency-wide ERM implementation. Which is best (part 2 Of 2)?
- Is ERM only applicable at the departmental level?
- What thoughts do you have on rationalizing and aligning the concepts and terminology of the internal control community with the risk management community?
- I am drafting a risk assessment report and want to understand whether exclusion of current risk reports should be excluded. Am I just identifying issues, or also giving credit for planned or in process work?
- Do you know of a repository for risk management specialist position descriptions?
- How many small and large Federal agencies have ERM?
- After compiling the risk register, how do you score the risk? How do you score the claimed effectiveness of mitigation?
- Considering the current market for Federal ERM professionals, would it be highly unlikely to find a 10-year professional within a salary range of \$95k – \$105k?
- I have yet to hear of anyone's risk profile, including my own, that includes opportunities, even though A-123 requires risk profiles to include opportunities. Why is that?
- How do you maintain precise risk trigger descriptions when you aggregate risk profiles from low organizational levels to higher level summary risks? It becomes difficult to know which trigger event is monitored to determine when a risk response should be executed.
- The COSO ERM – integrated framework identifies three approaches to communicating an organization's risk appetite (e.g., through general statement,

Thought Leadership for the Federal Enterprise Risk Management Community

by organization objectives, or by risk types identified by the organization). What organizational characteristics would benefit from each of these methods?

- How can the OIG's risk assessment process for audit planning purposes coexist with the ERM program's assessment for risk management purposes? Where is the line drawn for collaboration?
- How will auditors audit ERM, since this is different than regulation and procedure compliance? What conversations are happening with IGs to ensure they understand how ERM works?
- Where should the ERM process/program reside within the agency to include who should oversee the program?
- If agency executives view ERM as an administrative burden, what's the best way to approach ERM at that agency?
- How long does it take to implement a fully compliant ERM program?
- What are some effective methods to report the status and/or results of ERM activities to management?
- How do you consider existing controls in establishing the likelihood of the risk? Are risk responses by default internal controls?
- Of those ERM programs that have a formal communications program, what does it look like?
- Should agencies automatically focus resources on risks with the highest levels of residual risk, or should more energy be placed on those that may exceed established risk tolerances (regardless of residual risk level)?
- What are some techniques to leverage ERM information for the strategic objective review (SOR) process?
- What are some methods/strategies for promoting a healthy risk culture across the agency?
- What are some common strategies to identify and assess emerging risks or risks with a longer horizon?
- What are some proven methods to generate more active involvement of stakeholders in ERM efforts?
- What is the difference between a challenge and a risk?
- How can Chief Risk Officers (CRO) and ERM practitioners support cyber risk professionals to integrate existing cyber risk management models into the overall framework?

Thought Leadership for the Federal Enterprise Risk Management Community

- How can ERM help bring value and insight during the strategic planning process?
- I am a recent college graduate and am trying to gain more information on the world of risk management. What information would be helpful for a young adult with a finance degree and specialization in insurance/risk management. I have been reading up on ERM frameworks and am currently working in a claims role. There is extensive information out there and have no idea where to look.
- The benefits of ERM are often difficult to quantify. Are there measures or common practices to convey the value of ERM in more quantifiable terms?
- Private sector businesses often play a balancing act between company profit and insolvency risk. Is it necessary to perform similar analysis as part of a public sector ERM program, and how would that analysis differ?
- How does the application of ERM differ in making risk mitigation decisions vs. routine decision making?
- What methods can agencies use to identify risks that are not already realized problems?
- What are some of the top challenges facing agencies in integrating the OMB A-123 ERM framework with strategic objectives and decision-making processes?
- How can the agency ERM process and risk appetite principles be used to assist in mitigating strategic (long-term) risks resulting from COVID-19?

Join the ERM discussion at AFERM's Ask the Experts blog - www.aferm.org/ask-the-expert/.

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM's Communities of Interest/Practice

Supporting Federal ERM areas of specialty

AFERM maintains three communities of practice/interest for small Federal agencies, data analytics, and cyber-ERM. For more information on any of the communities of practice/interest, please reach out to the contacts noted below.

Community	Description	Contacts
Cyber-ERM Community of Interest (CYBERCOI)	A community of Federal ERM and IT practitioners seeking to bridge communications cross agency ERM and cybersecurity risk management functions	Nahla Ivy, Chair, Nahla.Ivy@nist.gov Julie Chua, Co-chair, Julie.Chua@hhs.gov
Data Analytics Community of Practice (DACOP)	A community of public sector ERM practitioners focused on advanced and applied data analytics supporting the evolution and maturity of agency ERM programs	Curtis McNeil, Chair, curtis.mcneil@aoc.gov LaTaiga B. Proctor, Co-chair, Lataiga.B.Proctor@census.gov
Small Agency Community of Practice (SACOP)	A venue for smaller agencies to share best practices and resources on ERM and a forum to discuss common challenges, provide learning opportunities, and foster networking and collaboration	Marianne Roth, Chair, Marianne.Roth@cfpb.gov Tal Seaman, Co-chair, tseaman@navigatorsof.com AFERM.SACOP@gmail.com

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM's 2020 Federal ERM Survey Results

The latest Federal ERM survey results are available



Federal Enterprise Risk Management

2020 Survey Results

The 2020 Federal ERM Survey is Guidehouse's sixth annual survey in collaboration with the Association for Federal Enterprise Risk Management (AFERM). It is designed to provide federal managers and leadership with perspective on the current state and trends of ERM in the U.S. Federal Government.

[Read Our 2020 Survey Results](#)

[guidehouse.com](https://www.guidehouse.com)

For the 6th consecutive year, AFERM and Guidehouse collaborated in conducting a survey of Federal ERM practitioners for their insights into the current state of ERM. The online survey was conducted in May 2020, engaging government members of AFERM, Association of Government Accountants (AGA), and the Senior Executives Association (SEA). While all respondents received the same set of initial questions, subsequent questions followed one of two prescribed paths based on whether the respondent's organization had already implemented an ERM program. Survey responses were received from a total of 37 Federal organizations, including 15 Cabinet agencies. In many of these cases, respondents represented component agencies or bureaus.

This year's survey indicates ERM continues to be an emerging capability in the Federal sector, though incremental positive trends are evident across most of the areas measured. Additionally, as highlighted in previous surveys and again this year, several characteristics impact the effectiveness of ERM.

Thought Leadership for the Federal Enterprise Risk Management Community

The two demographic categories with the highest mean scores and most positive responses are:

- Organizations that incorporate risk management into the performance plans of all members of the Senior Executive Service (or equivalent); and
- Organizations with ERM programs that have been running for 3 or more years.

The two demographics categories that demonstrate a higher correlation for ERM effectiveness, albeit not as significant as the categories above, are:

- Organizations in which the ERM program reports directly to the Agency Head or Deputy; and
- Organizations with a CRO in charge of their ERM program.

These highlights along with additional observations and insights can be accessed on the 2020 Federal ERM Survey Results Dashboard. This year's survey report includes an interactive dashboard with demographic filters for the survey results and over 350 visualizations for the 2020 and 2019 data.

The survey results is accessible via Guidehouse's website at guidehouse.com/insights/advanced-solutions/2020/aferm-survey-results-2020 and via AFERM's website at aferm.org/about/surveys.

For more information on the annual ERM Survey, please contact **Kate Sylvis**, Director, Risk Consulting, Guidehouse at ksylvis@guidehouse.com, and **Ken Fletcher**, AFERM President, at President@AFERM.org.

Thought Leadership for the Federal Enterprise Risk Management Community

An aerial photograph of a city street intersection with a large green and grey graphic overlay. The text "The Future of Consulting Lives Here" is centered on the green area. A white text box is positioned in the bottom right of the graphic.

**The Future
of Consulting
Lives Here**

We are Guidehouse. We help commercial and public clients address their most important challenges with innovative solutions that advance conventional thinking and create value for their stakeholders, build trust in society and shape a new future.

Follow Us Online **@Guidehouse**

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM Membership

Membership provides access to valuable ERM resources

With around 600 members, AFERM serves the Federal government and the public through sponsoring efforts for full and fair accountability for managing risk in achieving organizational objectives. AFERM maintains a forum for discussion of government ERM, sponsoring educational and training programs, encouraging professional development, influencing risk management policies and practices, and serving as an advocate for the profession.

Benefits of AFERM membership include the following:

- Education, training, and knowledge
- Insights on emerging trends, tools, and techniques
- Career advancement and networking opportunities
- Direct access to risk management professionals in the public and private sectors
- Annual Federal ERM Summit for advancing industry best practices

To join AFERM, please use the following link: <https://www.aferm.org/membership/>.

The chair of the AFERM Membership Committee is **Yehuda Schmidt** of Cotton & Company at Membership@AFERM.org.



No open season needed
Life insurance on your time.
Visit waepa.org

WAEPA
Group Term Life Insurance
Serving Civilian Federal Employees Since 1943

Thought Leadership for the Federal Enterprise Risk Management Community

Thought Leadership

Integrated Technology Solutions to Automate Your Agency's ERM Program

By Soumya Chakraverty, Managing Consultant, Risk Pro Solutions, and Nicole Puri, Chief Risk Officer, Bureau of the Fiscal Service

Are you responsible for your agency's implementation of Enterprise Risk Management (ERM)? Do you have questions about how to apply automation to ERM to streamline your work and make it more productive? In this article we will talk about the benefits of automating your ERM work, including what problems it can solve, and how to get the most out of automation.

Automation within ERM typically means leveraging technology solutions, such as those offered by an enterprise Governance Risk and Compliance (eGRC) solution. However, automation of ERM is not just a technology project; it incorporates a holistic approach, including assessing process and data maturity, organizational readiness, scoping, roadmap development, technology selection, and implementation program management. When it comes to deploying technology in Federal ERM, there is a lot of interest but also many questions. This article focuses on addressing some of these common questions, and shares approaches for ERM automation through an *integrated technology solution*.

ERM Pain Points and Automation Benefits

Automation can assist with a number of pain points in implementing ERM processes.

Pain Point	Automation Benefit
<p>Risk visibility and reporting In many agencies, a lack of visibility across components or bureaus may mean risks or connections between risks are being missed.</p>	<ul style="list-style-type: none"> • Common enterprise risk repository • Enables improved risk aggregation across the enterprise (left-right) as well as bottom-up • Agencies gain visibility into risk, root causes, and risk connectedness between and among components. • The ability to aggregate risk by a common risk taxonomy, or risk language. This can be an automation of existing taxonomies or a new effort to align the agency's usage of risk terms with their practice of risk management
<p>Lack of risk accountability SharePoint and Excel are easy to use and widely available, but they cannot easily accommodate automation.</p>	<ul style="list-style-type: none"> • Automated eGRC solutions have built-in capabilities to align risk and controls data to business entities, processes, and accountable executives. • Individualized risk reporting by accountable official, and for multiple accountable officials. For instance, automated tools can generate dashboards, heat maps, and other visual reports showing progress in each official's area of responsibility • They can also automatically generate notifications to responsible parties to help in the proactive management of risk across all layers of the agency

Thought Leadership for the Federal Enterprise Risk Management Community

Pain Point	Automation Benefit
<p>Tracking and managing root causes The process of identifying root causes of risk across any agency can be complex and manual.</p>	<ul style="list-style-type: none"> • The ability to associate, track and manage root causes and impacts across both small agencies and large, complex agencies with multiple components or sub-agencies. • Further, for risks that can be managed through internal controls, automation can help an agency understand how internal controls can mitigate the risk drivers, increasing the interconnected between ERM and Internal Controls as required in OMB Circular A-123.
<p>Managing large volumes of inter-connected risk data Even for small agencies with few risks, the volume of risk data can become unwieldy when linked to other data and to internal controls.</p>	<ul style="list-style-type: none"> • Maintain a single organizational risk repository, with multi-dimensional relationships between different data elements. • In-built security controls limit access to view and edit data on a need-to-know basis.
<p>Duplication of effort and data Without insight to the processes and controls across every part of an agency, there will be duplication of effort and data.</p>	<ul style="list-style-type: none"> • All risks and controls co-located in the enterprise risk repository helps detection of duplicative processes and controls which may be employed across multiple parts of the agency. • Consolidated risk reporting promotes greater transparency around risk and reduces inefficiencies due to data redundancies.
<p>Resource intensive Managing risk data collection and reporting is a manual effort for most agencies.</p>	<ul style="list-style-type: none"> • Automates resource-intensive data collection tasks • Enables efficiencies (such as workflows), reduces costs, and allows risk resources to be deployed to analysis rather than transactional activities.

What should an agency consider when contemplating an automation effort?

Readiness: Your agency's readiness for automation, especially its organizational and process maturity, should drive when the program is initiated. One key to keep in mind is the number of programs in the initial scope, as this can significantly increase complexity. A maturity assessment at the onset can help identify priority areas for initial deployment. Integration of the remaining programs can be done in stages across multiple phases of deployment and can span multiple years.

Executive Sponsorship and Funding: Consider the need for executive sponsorship for the technology. An ERM implementation is not a bottom-up exercise. Getting buy-in from senior decision makers early on and securing support and funding for the initiative during the appropriate budget year planning, is a key to its success. Preparing a business case to show how the automation fits in to the agency's strategic goals, how it can streamline operations and save money, and what the expected cost is to maintain the solution over time can be a good way to obtain executive support and understand how the effort fits in with other priority spending.

Thought Leadership for the Federal Enterprise Risk Management Community

Key Personnel Dependencies: The implementation of an integrated technology solution for ERM requires support of key people with specific skillsets, such as risk managers, technical SMEs, process specialists, etc. Though a continual challenge for many agencies, it is essential to understand these key dependencies, and continue to attract, retain, and motivate top talent to support the program. If these skills are not available within the agency, then it should be appropriate to look for them outside.

What Capabilities is Your Agency Looking for in an Integrated Technology Solution?

Many risk areas can be automated. Before deciding to implement any capability, carefully analyze the business requirements and the functionality offered by different tools. For context, here are some of the common functionalities that organizations typically deploy through an integrated technology solution:

- **Risk and control matrix** - Integrated technology solutions provide automation capabilities for RCMs by creating system inventories for risks and controls, as well as automating the data collection through online templates, surveys, and questionnaires. Risk and control rating scales can be configured within the solution to automatically calculate risk exposure based on survey results and other parameters. Integrated workflow capabilities within the solution allow tasks to be routed to assignees, track these to completion, and route results to leadership for approval.
- **Risk monitoring and mitigation action planning** - Provide capabilities for ongoing monitoring of risk and controls through key indicators (e.g. KRI, KPI, KCI etc.). Depending on the configured risk tolerance thresholds, the solution should also have the capability to generate automated alerts and action plans that lead to mitigation activities for risk reduction.
- **Controls testing and monitoring** - Streamline control testing by maintaining testing calendars, automated test programs and plans. Workflow capabilities support assignment of testing tasks, capturing and approval of test results, and generation of issues for exceptions. Most solutions also provide integration capabilities with other continuous controls monitoring (CCM), robotic process automation (RPA), or other automated testing solutions, for seamless integration and reporting of test results.
- **Issue management** - Support end-to-end issue management, starting from capture and triage, root cause analysis, identification and assignment of remediation actions to relevant personnel, and tracking these to closure. For operational events or incidents, these automated solutions support event logging, containment actions, and analysis of lessons learned.
- **Policy governance** - Central to risk governance is the development and management of enterprise policies, standards and procedures. Policy management functionality provides a centralized repository, as well as workflow

Thought Leadership for the Federal Enterprise Risk Management Community

capabilities to enable periodic review, update, and retirement of all enterprise policy documents, to verify that these are relevant and current at all times.

- **Compliance management** - Maintain compliance with laws and regulations, as well as internal policies and standards by providing library capabilities to track requirements and obligations, and assign their applicability to organizational processes, risks and controls. Integrating compliance management with ongoing risk management helps to ensure that compliance matters are not handled in silos; instead, there is coordination among relevant stakeholders (i.e. General Counsel, ERM, business units, Chief Financial Officer) to assess impacts of regulatory changes, understand applicability, and ensure that appropriate controls and monitoring activities are in place.
- **IT risk management and cybersecurity** - Automated tools support and manage technology asset inventories, conduct risk and control assessments, security incident response, and continuous monitoring. In recent years, more unique capabilities have been offered by different tool vendors to support Supply Chain/Third Party Risk Management (TPRM) as well as Business Continuity Management (BCM) processes. Although these are often considered extensions of IT Risk Management, TPRM and BCM can also be implemented as standalone solutions.
- **Enterprise risk management** - Enable automation of several ERM functions, including an assessment of enterprise-level risks, risk appetite, risk scoring, and key risk indicators.
- **Audit management** - Support all aspects of the audit lifecycle, including planning, scoping, risk assessment, audit execution (testing and workpaper management), and recording and reporting of audit findings.

Criteria for Selecting an Integrated Technology Solution

When your agency is ready to automate, and you are in the market for a technology solution, carefully consider the capabilities offered by each solution and how they will address your business requirements. Often a technology solution is selected based on references, or because it has successfully worked somewhere else. Keep in mind, one solution does not fit all. Below are several criteria to consider:

- **Functionality and extendability** - The suitability of a technology solution is dependent on how well it supports the agency's ERM processes. Most solutions come pre-packaged with a set of data elements, screens and workflows that can be configured based on organizational needs, and which offer capabilities for extending functionality.
- **Usability** - A key success factor in the adoption of an integrated technology solution is its usability. Usability is impacted by certain factors such as ease of navigation (including breadcrumbs), screen layout, workflow, global search

Thought Leadership for the Federal Enterprise Risk Management Community

capability, intellisense (i.e. auto-completion of search parameters), and navigation history.

- **Solution compatibility** - Like any application, it is critical that the deployed solution is compatible with the agency's technology architecture. While integrated risk technology solution vendors support on-premise and cloud-based deployment, consider whether the solution you are evaluating is available only as Software-as-a-Service (SaaS), where software is accessed online via a subscription, or whether it can be deployed within the organization's internal network.
- **Vendor support** - An integrated technology solution implementation can require extensive business and technical consultation and support. The vendor's ability to support the implementation with business and technical consulting, as well as user training, is key. Without it, users can incur hidden costs to achieve basic functionality.
- **Reporting and analytics capabilities** - Some of the leading trends in analytics capabilities, which your agency may want to have include risk aggregation, "what if" risk scenario analysis, predictive analytics, and machine learning, including natural language processing or other artificial intelligence (AI) capabilities.

Conclusion

Automating functions within your ERM program, particularly when you include functionality for internal controls, can address many of the pain points agencies face today including lack of visibility; tracking risk, root causes and other information across silos; and better management of data and resources. Carefully consider where your agency is in its path to ERM maturity before moving forward with implementation of any technology; lack of maturity in processes or understanding of scope can create problems which may limit the success of the implementation. Finally, take the time to learn about what technology offers and how that matches up to your agency's needs. Just like with any technology implementation, budget, overall functionality, usability within the existing technology framework of the agency, vendor support options and potential for including new and developing technologies should be planned. With a successful integrated technology solution, your agency can be more efficient in both its compliance efforts and its risk management implementation.

Soumya Chakraverty is a managing consultant at Risk Pro Solutions. A senior risk management professional, he specializes in ERM, regulatory compliance, controls design, and integrated risk technology solutions. He regularly provides consulting services on risk integration and maturation. A regular public speaker, he has also published articles on GRC implementations and operational risk.

Thought Leadership for the Federal Enterprise Risk Management Community

Nicole Puri is the Chief Risk Officer for the Bureau of the Fiscal Service. She leads the Bureau's implementation of Enterprise Risk Management under A-123. She has previously served as the Risk Management Officer for the Pension Benefit Guaranty Corporation and the Deputy Director of the Enterprise Risk Management Division for the Office of Public and Indian Housing at the Department of Housing and Urban Development. Ms. Puri has also advised Federal clients on ERM, fraud risk management and integrated risk management efforts previously as a Director at KPMG. She has published several articles on risk management topics and holds a law degree from George Mason University School of Law. The views and opinions expressed in this article are solely her own and do not necessarily reflect those of any Federal agency, entity or instrumentality, including the Bureau of the Fiscal Service, or the United States.

Soumya Chakraverty may be reached at schakraverty@riskprosolutionsllc.com and **Nicole Puri** may be reached at nicole.puri@fiscal.treasury.gov.



Thought Leadership for the Federal Enterprise Risk Management Community

AFERM's 2021 Board of Directors

New Board of Directors Announced

On September 13th at the AFERM 2020 Summit, AFERM announced its 2021 Board of Directors, which is effective on October 31st. AFERM's incoming president Nicole Puri noted that “[i]t is both an exciting and uncertain time to start my tenure” and “[w]ith change comes opportunity, and AFERM is ready to move forward both on key initiatives to offer more value to its members and sponsors, as well as to expand the value that ERM provides to the mission success of government agencies. I look forward to an innovative and challenging year as AFERM President, and thank our members and volunteers for the opportunity to lead this great organization.”

The 2021 AFERM Board of Directors includes:

- President: [Nicole Puri](#), Bureau of the Fiscal Service
- President-Elect: [Daniella Datskovska](#), Guidehouse
- Past-President: [Ken Fletcher](#), Kestrel Hawk Consulting
- Secretary: [Thomas Holland](#), Guidehouse
- Treasurer: [Doug Webster](#), AFERM Co-Founder and Independent ERM Advisor
- VP-at-Large: [Harold Barnshaw](#), Office of the Comptroller of the Currency
- VP-at-Large: [Alice Miller](#), Development Finance Corporation
- VP-at-Large: [Sean Vineyard](#), 11th Hour Service

AFERM wishes to express its gratitude for the leadership of the 2020 Board, including Ken Fletcher who served as the 2020 AFERM president and will continue on the Board as past-president for 2021.

Thought Leadership for the Federal Enterprise Risk Management Community

Mission-Driven Security

Achieving Successful Cyber Outcomes

RSA delivers Mission-Driven Security so organizations across the Public Sector can take command of their evolving security posture.

Learn more: <http://www.rsa.com/publicsector>



RSA

Thought Leadership for the Federal Enterprise Risk Management Community

2020 AFERM Officers, Committees, and Communities

PRESIDENT



Ken Fletcher

PAST PRESIDENT



Tom Brandt

PRESIDENT-ELECT



Nicole Puri

SECRETARY



Thomas Holland

TREASURER



Fola Ojumu

TREASURER-ELECT



Doug Webster

VP AT LARGE



Harold Barnshaw

VP AT LARGE



Sean Vineyard

VP AT LARGE



Alice Miller

Thought Leadership for the Federal Enterprise Risk Management Community

Audit

Alex Ng, Chair

Communications

Shelly Turner, Chair
Nadya Korobko

Finance/Budget

Fola Ojumu, Chair

Infrastructure and Operations

Ed Hau, Chair

Knowledge Capital

Brian Murphy, Chair
Tim Weber

Membership

Yehuda Schmidt, Chair
Domenyck Schweyer

Outreach and Advancement

Sean Vineyard, Chair
Cynthia Vitters, RIMS Liaison

Planning

Christina Girardi, Chair
Marc Pratta, Co-chair

Programs

Varun Malhotra, Chair

Summit 2020 Planning

Meredith Stein, Chair
Marianne Roth, Co-chair

Volunteers

Irena Marchand, Chair
Janice Ho, Co-chair

Cyber ERM Community of Interest

Nahla Ivy, Chair
Julie Chua, Co-chair

Data Analytics Community of Practice

Curtis McNeil, Chair
LaTaiga Proctor, Co-chair

Small Agency Community of Practice

Marianne Roth, Chair
Tal Seaman, Co-chair

Corporate and Associate Advisory Group (CAAG)

Platinum Sponsors

Sean Vineyard, 11th Hour Service
Cynthia Vitters, Deloitte LLP
Chris Hare, Ernst & Young
David Fisher, GuideHouse
David Zavada, Kearney & Company
Tim Comello, KPMG LLP
Carrie Everett-Vaughn, RSA

Gold Sponsors

Bobbie-Jo Pankaj, Grant Thornton

Silver Sponsors

Simone Reba, Accenture Federal
Jeannine Rogers, AOC Solutions
Stephanie Irby, BDO
Bert Nuehring, Crowe LLP
Jillian Campbell, Galvanize
Tim Mobley, IRIS Intelligence
Shawn O'Rourke, Pro-Concepts
George Fallon, RMA Associates, LLC
Sim Segal, SimErgy Consulting
Tashu Trivedi, TFC Consulting, Inc.
Paul Marshall, The MIL Corp
Celine Serrano, WAEPA
Jay Colavita, Workiva/Vertosoft

CAAG Liaison

Soumya Chakraverty

Thought Leadership for the Federal Enterprise Risk Management Community

RIMS-CRMP-FED Certification



RIMS-Certified Risk Management Professional for Federal Government Credential

The RIMS-CRMP-FED is a credential that was developed in cooperation with the Association for Federal Enterprise Risk Management (AFERM). It distinguishes the achievement of validated risk management competencies for an effective risk professional in the federal government. Individuals who earn the RIMS-CRMP-FED have demonstrated their knowledge and proficiency in the area of risk management in the U.S. Federal Government, and are dedicated to upholding high standards of ethical and professional conduct.

Benefits

- Prove your knowledge of risk management competencies.
- Demonstrate your commitment to the profession by adhering to a strict Code of Ethics and meeting continuing education requirements.
- Enhance your professional reputation and gain a competitive advantage.

Eligibility

Degree and Experience Requirement

- Bachelor's degree or higher (or global equivalent) in risk management, and
- One year of full-time work experience (or full-time equivalence) in risk management*

OR

- Bachelor's degree or higher (or global equivalent) in non-risk management area of study, and
- Three years of full-time work experience (or full-time equivalence) in risk management*

Note: Degrees must be obtained from accredited or equivalent schools of higher education. Internships count toward risk management experience.

Non-Degree Experience Requirement

- Seven years of risk management experience*
- Possessing the Associate in Risk Management (ARM) counts towards two years of risk management experience.

Examination

The RIMS-CRMP-FED exam is two parts: the core RIMS-CRMP exam and the FED exam. The computer-based exam is three hours and comprises 170 questions. It addresses five risk management competencies and three federal domains:

- Analyzing the Business Model
- Designing Organizational Risk Strategies
- Implementing the Risk Process
- Developing Organizational Risk Competency
- Supporting Decision Making
- Understanding the Federal Government Risk Management Environment
- Risk Management Implementation in the Federal Government
- Risk Management Reporting in the Federal Government

How to Earn the RIMS-CRMP-FED

- Meet the eligibility requirements.
- Apply online at www.RIMS.org/Certification.
- Receive approval to take the exam.
- Schedule an exam date during your six-month authorization period.
- Take the exam at a Pearson VUE Testing Center. Visit www.PearsonVUE.com/RIMS to find a testing center.
- Pass the exam to become a RIMS-CRMP-FED.

*Risk Management Experience is occupational experience that leverages the opportunities and uncertainties associated with an organization's goals and objectives. This includes implementing, developing or leading the risk management practices that enable an organization to make risk-effective decisions that create and sustain value.

Learn More and Apply Online | www.RIMS.org/Certification



Thought Leadership for the Federal Enterprise Risk Management Community

Corporate Sponsors and Partners

Thank you for your support!

Platinum Sponsors



Gold Sponsors



Silver Sponsors



Thought Leadership for the Federal Enterprise Risk Management Community



Educational Development and Community Partners

