AFERM
Association for Federal Enterprise Risk Management

AFERM Newsletter

Issue 32
March 2020

Thought Leadership for the Federal Enterprise Risk Management Community

Contents

Highlights

This 32nd issue of the quarterly AFERM Newsletter includes thought leadership articles from ERM practitioners with Crowe, Deloitte, RMA Associates, and RSA. Also, AFERM's 2020 Summit will be virtual and the date has been moved up to September 10th – a full day of connectivity, idea sharing, and continuing professional education, with the risk of COVID-19 minimized.

AFERM Association for Federal Enterprise Risk Management

AFERM Newsletter

Issue 32
March 2020

Thought Leadership for the Federal Enterprise Risk Management Community

The President's Corner

AFERM President Ken Fletcher

The value of enterprise risk management (ERM) to agencies operating in the wake of COVID-19

By Ken Fletcher, AFERM President

The on-going public health crisis directly impacts AFERM as it affects all federal agencies. Perhaps the largest impact on the association is on our planning for the 2020 AFERM Summit. On behalf of AFERM's Board of Directors, I want to thank the members who responded to the Summit survey and for sharing your comments. More than half of the respondents indicated a preference to shift to a virtual Summit. Your inputs informed the Board's deliberations during the April meeting. Because of the uncertainties concerning how the virus might impact the National Capital Region in late October and the increasing financial impact on AFERM, the Board unanimously decided that the 2020 Summit will be a virtual event. The Board also approved moving the date for the Summit to September 10th and lowering the registration fee. More details will be provided by our Summit Planning Committee Chair and Vice-Chair, Meredith Stein and Marianne Roth, as they shift their focus to an on-line Summit agenda.

That said, I want to focus this President's Corner on the potential opportunities presented by the current public health crisis and the potential value of ERM across four (4) time frames: Immediate, short-term, intermediate, and long-term. The impact of the on-going COVID-19 pandemic is disruptive and requires us to adapt in both our professional and personal lives. Understandably, the current focus of government and society is on mitigating the systemic risk to public health and the economy. As the virus began disrupting global supply chains and then the core functionality of agencies and businesses, several articles were published about how ERM principles can help organizations navigate through the hyper-uncertainty of this global health and economic crisis. There is clearly a role for agency ERM functions in supporting leadership during this crisis, and part of that role is helping understand the adverse impacts and developing response actions.

Quite naturally agencies are concentrating on the threats posed by this risk. From necessity, nearly every organization is being forced to change the way they conduct

business from converting to wide scale telework to changing how goods or services are delivered to their customers. Continuity of operations plans and information technology systems are being stress tested and enterprise risks identified as a direct result of this low-probability high-consequence event. However, as reflected in the government's definition, risk can also present an opportunity. As Niccolò Machiavelli is reported to have said, "Never waste the opportunity offered by a good crisis."

On March 2nd, McKinsey & Company began posting a series of informational articles to provide insights into the implications of COVID-19 for businesses (available at https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-implications-for-business). While these articles focus primarily on private sector businesses, I find several of their insights very useful for government agencies and ERM functions. One particularly beneficial article from March 30th discusses five broad planning perspectives reflecting the immediate, recovery, near-term, intermediate and long-term horizons, referred to by the authors as the "5Rs." They are Resolve; Resilience; Return; Reimagine; and Reform. From an agency perspective, the ERM function can help identify and manage potential risks that may exist from planning for recovery through the long-term. The crisis also presents the potential opportunity to accelerate and apply new capabilities and advance aspects of the ERM program to the advanced or strategic levels of maturity.

Recent comments from public health officials indicate two broad areas of concern: 1) Resurgence of the virus immediately after current mitigation measures are relaxed; and 2) Subsequent waves of the virus this fall and until a vaccine is available. These concerns span the immediate and short-term time horizons and the associated risks to agencies.

ERM principles and approaches are valuable during the immediate phase in identifying the potential key risks the agency may confront and developing agency response actions for those risks. Several different articles I have read recently identify potential recovery risks related to the following:

- Managing vulnerable employee populations
- Accommodating employees with vulnerable family members
- Preventing introduction of the virus into the workplace
- Establishing and enforcing workplace social distancing
- Addressing sanitization and cleaning of the workplace

ERM principles and approaches are equally applicable to the short-term time horizon for helping posture the agency for better preparedness in responding to anticipated future waves of COVID-19. Within this time horizon, ERM functions can help agencies address potential risks to include mitigating the impact and/or likelihood of a repeat of major challenges encountered during the short-term wave and mitigating the impact of pandemic response outcomes with potential enduring negative effects on the agency.

Pursuing potential opportunities present over the intermediate and long-term horizons increases value to agencies; and, similarly, the potential value and contribution of the ERM program also increases during these time frames. Key risk opportunities in intermediate and long-term time horizons include:

- Strengthening agency resiliency
- Streamlining / reengineering processes to increase operational efficiency and cost-effectiveness based on lessons learned from the crisis
- Understand the linkage and dependencies between the external risk environment (such as supply chain risks) and the agency's risk profile
- Improving agency crisis management capabilities and COOP operations
- Identifying activities that can be stopped or reduced to re-purpose agency resources
- Realigning mission critical systems, mission critical functions and resource allocations to these critical areas

Beyond the broader opportunities this crisis presents at the agency level, it presents specific opportunities for agency ERM programs to realize a discontinuous shift in their maturity curve and to increase the value the program provides agencies through the following:

- Accelerating ERM program capabilities (i.e., earlier adoption of scenario planning and risk modeling)
- Implementing/improving agency risk appetite statements, risk tolerances, and risk limits
- Developing a broader set of key risk indicators (KRI) working in alignment with agency key performance indicators (KPI)

Thank you for the honor of serving as President of this wonderful Association. I hope each of you and your loved ones remain safe and healthy during these trying times.

All the best,

Ken

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

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
- **James Ansberry**, Senior Manager, and **Bert Nuehring**, CPA, CGMA, Partner, Crowe
- **Seth Malaguerra**, Manager, and **Alyssa Jackson**, Senior Consultant, Deloitte & Touche LLP
- **George Fallon**, Director, and **Devin Borden**, Manager, RMA Associates
- **Marshall Toburen**, Risk Management Strategist, and **Dan Carayiannis**, Public Sector Director, RSA

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@guidehouse.com and nkorobko@guidehouse.com, respectively.

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
ERM Virtual Workshop: Driving Organizational Value-Enhancing Performance	AFERM & AGA	June 15	Virtual
SIMERGY: 10th Annual ERM Boot Camp	SimErgy	June 15-16	Virtual
Prescient: The Foresight Sandbox	Prescient & Arizona State University	June 15-17	Washington, DC
RIMS-CRMP-FED Prep Workshop	RIMS	August 27-28	Arlington, VA
2020 AFERM Virtual ERM Summit	AFERM	September 10	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.

Thought Leadership

Engaging stakeholders: Promoting ERM as more than a compliance exercise

By James C. Ansberry, Senior Manager, and Bert G. Nuehring, CPA, CGMA, Partner, Crowe

Federal agencies have been required by OMB to implement ERM for several years, but many have struggled to overcome their stakeholders' skepticism toward the program.

Stakeholders often tend to regard ERM as nothing more than another burdensome compliance exercise that should be a priority only for those charged with the program's governance. The challenge for chief risk officers (CRO) or chief financial officers (CFO) is to obtain buy-in and educate all levels of their agencies on the ongoing importance and benefits of ERM and how their participation affects it.

The ERM requirement

The 2016 update to OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, imposes the ERM requirement. The update reflects OMB's realization that government operations have undergone significant changes since the circular first published in 1981. Among other developments, technology has made dramatic advances, and expectations related to government accountability have intensified. The ERM requirement was designed to address such shifts by improving mission delivery, reducing costs, and better focusing corrective actions.

The OMB defines ERM as an agency-wide approach to addressing the full spectrum of the organization's external and internal risks – including financial, strategic, and reputation risks – by understanding the combined impact of risks as an interrelated portfolio. ERM gives an enterprise-wide, strategically aligned portfolio view of risk that provides greater insight on how to most effectively manage risks to achieve successful mission delivery. While OMB concedes that agencies cannot respond to every risk related to achieving strategic objectives and performance goals, it expects agencies to identify, measure, and assess risks related to mission delivery.

For the naysayers among the stakeholders, though, such language fails to communicate the on-the-ground advantages – in other words, what's in it for them. It is up to leadership (typically the CRO or CFO) to help them understand why they should dedicate their time and limited resources to aid in building a robust ERM program. Perhaps the most effective strategy to get stakeholders on board with ERM is to highlight how the data and information collected and analyzed through the program can help them in their own roles.

Budget development and funding requests

Ideally, stakeholders will come to view ERM as a way of uncovering risks that are not being properly managed and use the data to make the case for more personnel, systems, software, and processes to effectively manage those risks. Risk data could inform the annual budgeting process (for example, resource allocation planning in the Department of Homeland Security (DHS) or planning, programming, budgeting, and execution in the Department of Defense) or when making unfunded requests.

In fact, ERM programs produce critical evidence, data, and supporting documentation for justifying all sorts of proposed solutions for both internal and external problems. For example, the individuals spearheading a departmental or agency reorganization can use the information to develop the new structure and the requisite business plan. Considering the relevant portfolio of risks identified by ERM can improve the odds that the new structure is well aligned with risk management. It might, for instance, steer the reallocation of staff time to higher-risk priorities and tasks.

Efficiency improvements

An ERM program can help agencies identify and prioritize the mitigation activities and controls that they could automate and make more efficient by implementing systems, software, data analytics, artificial intelligence, robotic process automation (RPA), and machine learning.

For example, an agency might have one or more employees who currently consume a lot of time manually combing through spreadsheets to clean and analyze data. An employee might have the bandwidth to audit only 10% of a sample of listed transactions, but an RPA running 24/7 potentially could audit the entire data set and send potentially noncompliant records for review and correction. Post-automation, those personnel can be redirected to higher-priority tasks, which supports a Cross-Agency Priority goal of the President's Management Agenda – shifting the federal workforce from low-value to high-value work.[i]

In recent years, government employees have grown accustomed to being told they need to do more without any additional funding, staff, or other necessary resources. They likely will welcome the opportunity to automate certain processes and procedures while redirecting resources to manage higher risks. In addition, the funds saved through automation can be otherwise deployed to further an agency's mission.

The good news is that agencies can employ the best practices and lessons learned from other departments and agencies' established programs, processes, procedures, and systems. Stakeholders should find adopting (and tailoring) partner agencies' proven initiatives and measures less daunting than starting from scratch. An agency with a mature ERM program will be able to take advantage of opportunities for informed risk taking and strategic planning, understand their risk appetite and tolerance, have an open dialogue about risks, and align mission to strategy.

For example, DHS comprises multiple components, such as the U.S. Secret Service (USSS), U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE) – each of which has its own CRO or CFO. To identify industry best practices, CBP and ICE can refer to what USSS has done with its ERM program. Questions CBP and ICE could ask might include: Which systems, policies, and procedures does USSS have in place? What hurdles did it face in implementation? How did it overcome those hurdles?

The General Services Administration has taken some steps to encourage such sharing of information. In 2019, for example, it launched a community of practice (CoP) for RPA.[ii] The CoP is designed to allow federal government leaders to explore opportunities, share ideas, and collaborate on how they can effectively implement RPA in their respective agencies, including for risk management purposes. The community has grown to include representatives from dozens of agencies.[iii]

A more holistic approach

ERM programs are required for federal agencies, but merely mandating them is not enough to reap all the potential benefits. When the stakeholders in an agency see their ERM responsibilities as simply another box to check off and move on from, the ERM program will fall short. CROs and CFOs, therefore, must take the time to earn their stakeholders' buy-in. Explaining how the data and information can help stakeholders in their own roles will encourage them to become invested in a program they might otherwise see as tangential at best.

Jim Ansberry may be contacted jim.ansberry@crowe.com and **Bert Neuhring** may be reached at bert.nuehring@crowe.com.

[i] General Services Administration and the Office of Management and Budget, "Shifting From Low-Value to High-Value Work," Performance.gov, https://www.performance.gov/CAP/low-value-to-high-value-work/

[ii] Ed Burrows, "GSA Calls on Federal Emerging Tech Leaders to Form RPA Community of Practice," April 18, 2019, GSABlog, https://www.gsa.gov/blog/2019/04/18/gsa-calls-on-federal-emerging-tech-leaders-to-form-rpa-community-of-practice

[iii] U.S. General Services Administration, "2019 Agency Financial Report," accessed March 18, 2020, https://www.gsa.gov/reference/reports/budget-performance/annual-reports/2019-agency-financial-report/managements-discussion-and-analysis/performance-summary

AFERM's 2020 Virtual Summit

Register now to take advantage of early bird pricing

True to our risk management roots, AFERM's 2020 annual Summit is virtual this year. Scheduled for September 10th from 8:45 am to 4:45 pm, we offer five (5) continuing professional eduction (CPE) credits and a line-up of speakers to help bring ERM into focus with virtual plenary speakers, breakout sessions, and digital demonstrations.

This year's Summit Planning Committee is led by chair Meredith Stein of the National Institutes of Health (NIH) and co-chair Marianne Roth of the Consumer Fraud Prevention Bureau (CFPB).

Registration and Pricing

AFERM has again partnered with AGA on the Summit to handle registration through AGA's website. Check out AFERM's Summit website for instructions on registering. Registration pricing for early birds and AFERM members and non-members and speakers and moderators is summarized in the table below.

Registration Type	Early Bird (5/7 - 8/17/20)	Regular (8/18 – 9/10/20)
AFERM Members	$149	$189
Non-AFERM Members	$189	$229
Speakers and Moderators	$100	$100

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

AFERM's ERM Podcasts

AFERM's podcasts continue the ERM dialogue

This spring we made 11 podcasts – conversations with risk management professionals in the federal sector. The most recent podcasts cover a wide range of ERM topics:

- *Episode 25: 10 Years of ERM* – Dr. Karen Hardy, Director of Risk Management, U.S. Department of Commerce, on the evolution of ERM over the last 10 years.
- *Episode 26: The Costs and Benefits of ERM* – Vladimir Antikarov, Regional Director of the Professional Risk Managers' International Association (PRMIA) for Washington, DC, on calculating the costs and benefits of ERM.
- *Episode 27: AFERM Data Analytics Community of Practice (DACOP)* – Curtis McNeil, Risk Management Officer, Architect of the Capitol, and LaTaiga Proctor, Risk Management Officer, U.S. Census Bureau, on data analytics and ERM.
- *Episode 28: NIST Cyber Security* – Dr. Ron Ross, Fellow, National Institute of Standards and Technology (NIST), on upcoming updates to NIST Special Publications 800-37 and 800-53.
- *Episode 29: ERM at DOJ* – Lucy Mungle, Deputy Assistant Attorney General, U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), on OJP's ERM journey.
- *Episode 30: PBGC OIG* – Bob Westbrooks, Inspector General, Pension Benefit Guaranty Corporation (PBGC), on the Office of the Inspector General's (OIG) ERM program.
- *Episode 31: ERM at the CRA* – Brian Philbin, Assistant Commissioner and Chief Audit Executive, and Wendy Saschenbrecker-Tang, Manager, Canada Revenue Agency (CRA), on their ERM program.
- *Episode 32: ERM at the OCC* – Bill Rowe, CRO, Office of the Comptroller of Currency (OCC), on OCC's ERM program's start and integration with the agency's strategy.
- *Episode 33: AGA-ERM Workshop Lessons Learned* – Bert Nuehring, Partner, Crowe, Thomas Holland, Director, Guidehouse, and Sara Choi, Manager, Guidehouse, on lessons learned from the 2019 AGA-AFERM ERM Workshop and the 2020 Workshop.
- *Episode 34* – Paul Marshall, Vice President, The MIL Corporation, and Tal Seaman, Owner and Chief Executive Officer (CEO), Navigator Solutions, on their favorite podcasts.
- *Episode 35: Value-based Management* – Doug Webster, co-founder of AFERM and former federal government executive, on his new book, "Valud-based Management in Government."

Listen to these and other AFERM podcasts on our website at https://www.aferm.org/aferm-risk-chats/, and if you are interested in participating on a podcast, please contact Paul Marshall, MILCorp, and Tal Seaman, Navigator Solutions.

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

Thought Leadership

Enterprise risk response: Putting the "M" in ERM

By Seth Malaguerra, Manager, and Alyssa Jackson, Senior Consultant, Deloitte & Touche LLP

The risk response challenge

ERM provides federal agencies with a systematic process to facilitate improved decision-making, resource allocation, and strategic outcomes through a continuous cycle of identifying, assessing, prioritizing, and responding to risks. Many ERM programs designed to fulfill the requirements of OMB Circular A-123 (A-123) dedicate attention and resources to tools that support risk identification and assessment, such as risk taxonomies and assessment frameworks. While this is usually done to develop a comprehensive risk profile (i.e., one that includes all relevant types of risk), similar procedures to guide risk response activities are often missing. This can lead to ERM sitting on the sidelines during major crises or risk events, such as during the COVID-19 crisis, because ERM was disconnected from the management processes that the agency uses to manage events.

It does not need to be this way. Risk response guidelines in A-123 can be broken out along two dimensions. First, they recommend a broader set of response strategies to address risks, to include mitigating, avoiding, transferring, accepting, or even exploiting risk. Secondly, for risks that require mitigation, they provide more practical guidelines to manage these risks. This framework outlines a practical (or cross-functional) approach for precisely these kinds of risks – enterprise risks which are unacceptable and require mitigation. This framework, therefore, seeks to apply tangible, existing management activities to enterprise risks in a manner that is efficient, more comprehensive than may occur otherwise, and ultimately brings these risks to within appetite.

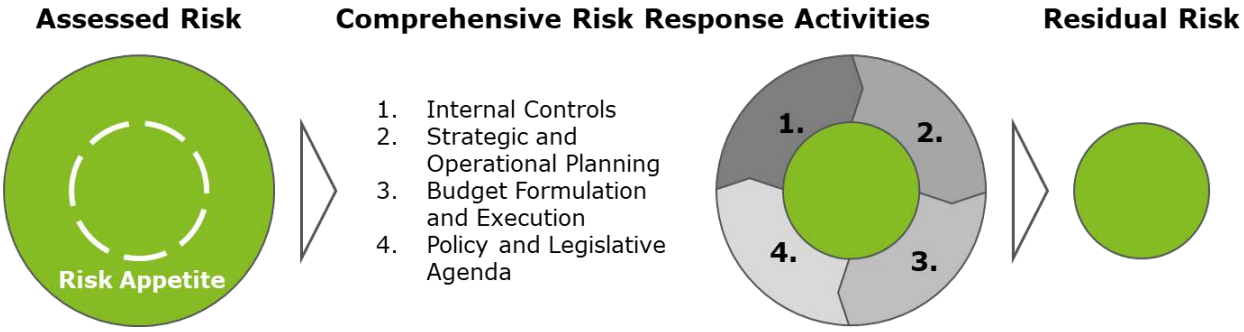
The importance of adopting a practical approach lies in establishing an effective organizational risk culture. Without an emphasis on risk response, ERM programs can easily become trapped in a cycle where enterprise risks are regularly identified, assessed, and prioritized, but little progress is demonstrated in addressing them. This lack of progress can create a negative feedback loop where ERM does not generate the buy-in necessary to sustain itself. In many instances, stakeholders may simply decide that the costs of participating in ERM exceed the benefits.

A practical risk response framework

A practical risk response framework as described here, aligns directly with ERM guidance in A-123, meeting its basic requirements, while providing a blueprint to improve risk response outcomes. The framework is centered on core management processes already used across the federal government – internal controls, strategic

planning (to include strategic reviews, performance management, and development of strategic or operational initiatives), budget formulation and execution, and the legislative and policy agenda. Often, risk programs only look to one of these elements, typically controls, in responding to risk. A broader risk response framework brings more tools from an agency's core management functions into the risk manager's toolkit.

Figure 1: Illustrating a practical, cross-functional risk response



These core practical risk response activities, as illustrated above, as a means of risk response, are described as follows:

- **Internal controls** can provide assurance that priority risks are actually under control (or identify specific weaknesses) through annual testing or evaluation activities, and they can provide continuous monitoring of major controls when the programs have that capability.
- **Strategic and operational planning** can include incorporating risk response directly into strategic and operational plans, addressing risk through new strategic and performance initiatives, and even changes to organizational design.
- **Budget formulation and execution** can be risk-informed so that the highest priority risks are also reflected as priorities when budgets are submitted to Congress and during budget execution processes, such as prioritizing and processing unfunded requests (UFR).
- **Policy and legislative agenda** can be similarly prioritized so that the highest profile risks are also prioritized for action via an agency's policy-setting branch and by shaping new legislation.

When determining whether to employ this framework, begin by considering whether a risk is outside of appetite or otherwise fulfills A-123 criteria to be mitigated or reduced. These are the risks most suitable for this framework. The first step is to determine whether the risk should be mitigated through internal controls, including if the risk

impacts control objectives or is high in likelihood and impact. Then determine if a new or refined strategic initiative (aligned with the agency strategic plan) could be impactful, if a legislative or policy change is required, or if the response activities require additional budgetary resources. Some agencies may be treating risk as part of their very mission through service delivery (e.g., Social Security Administration), grant making (e.g., Federal Emergency Management Agency), and/or regulatory or enforcement powers (e.g., the Food and Drug Administration and the Environmental Protection Agency). These should also be incorporated, as appropriate.

To make the framework more tangible, two risks from the GAO High Risk list are used as examples below. These were selected based on an assumption they appear in some form on risk profiles across the federal government. While these risks are associated more with business operations, this framework is just as suitable for priority mission-area risks or to aid in response and recovery from the COVID-19 crisis.

Example 1: Cybersecurity risk

Risk description. If the agency does not improve its cybersecurity posture, then government networks, critical infrastructure, and associated federal information will remain vulnerable to cyber-attack (in particular as more employees work remotely in the current environment). To address this risk, many federal agencies are taking a variety of actions, including better managing their cybersecurity risks and coordinating to meet reporting requirements related to cybersecurity of federal networks and critical infrastructure. A comprehensive response would include some of the below response tactics working together in an integrated and complimentary manner.

Management Process	Illustrative Response Examples – Cybersecurity
Internal Controls	• Define a role-based security model; annually evaluate and test roles-based permission or access models for high-priority information systems • Test and evaluate both internal and external reporting of cybersecurity incidents
Strategic and Operational Planning	• Add an objective to the strategic plan regarding information security • Establish information security technology investment review board to implement and monitor cyber projects and opportunities
Budget Formulation and Execution	• Fund upgrades and lifecycle replacements for legacy systems based on their vulnerability to cyber threats, as validated by cybersecurity control testing • Prioritize information technology unfunded requirements (UFRs) on the basis of achieving stronger cybersecurity posture
Policy and Legislative Agenda	• Implement an agency-level cybersecurity policy that aligns with the NIST National Cybersecurity Framework

Example 2: Human capital skills gap

Risk description. If the agency does not decrease the skills gaps in their workforce, then it will likely not be able to achieve mission in a timely and effective manner. To address this risk, the federal government has provided guidance, training, and on-going support for agencies on the use of data analytic methods for identifying skills gaps and the development of strategies to address these gaps.

Management Process	Illustrative Response Examples – Human Capital
Internal Controls	• Evaluate external hiring or internal staffing processes for operational efficiency • Develop control programs over special hiring initiatives, such as campus recruiting or special pay mentioned below
Strategic and Operational Planning	• Launch a campus or corporate recruiting program to boost hiring across critical skill areas • Create training cohorts for in-demand skills to build or develop required skillsets in the existing workforce
Budget Formulation and Execution	• Request an increase of XX FTEs for a new division in the office of operations for to improve timelines for critical skills hiring processes
Policy and Legislative Agenda	• Request special pay authority for critical skill positions to improve talent competition with the private sector or industry • Identify additional hiring authorities authorized for use by the agency in accordance with law and policy

As the final step, a residual risk assessment should be performed to complete the process and determine whether the response plan is effective and whether the risk is now acceptable. Because the activities in the practical framework typically occur in annual fiscal year cycles, it provides clearer starts and stops in the inherent-to-residual risk assessment process.

Conclusion: Adopting and implementing practical risk response

Everything described so far is done easily enough on paper. But how does such a response framework get put into practice? We recommend three foundational steps to getting started:

1. The organization's risk governance system should give appropriate stakeholders a seat at the table. This means including participants from both the mission and mission-support areas to help generate agency-wide responses. This should include strategy, performance, policy or legislative affairs, and internal control offices to move the risk council from just risk identifications to risk solutions.

2. Effective risk response requires effective planning. ERM should allocate planning resources to help ensure enterprise risk responses are well thought out and options have been evaluated for effectiveness and can be executed in an efficient manner.
3. The risk profile should capture and maintain all of the elements described above—in addition to risk assessment and prioritization—to provide a clearer picture of risk exposure and how the agency is responding to risk. A risk profile that also tracks a full range of practical risk response activities not only helps build confidence in leadership that their top risks are being addressed, it can also demonstrate how effectively these core management processes are producing desired mission and mission support outcomes.

Once the federal government transitions into the recovery phase of the COVID-19 pandemic, leadership is likely to pay renewed attention to ERM and similar resilience-building capabilities. Having a practical risk response framework is critical to providing ERM with a toolkit that can actually demonstrate results and thereby get ERM a seat at the table during these critical decision-making periods.

For inquiries please contact Seth Malaguerra (smalaguerra@deloitte.com); John Basso, Government and Public Services ERM (jobasso@deloitte.com); and Cynthia Vitters, Leader, Government Public Services ERM leader (cvitters@deloitte.com).

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:

- Three Grand Challenges For Government
- Supply Chain Under Strain
- Fighting Coronavirus Phishing Scams
- Lessons From China's COVID-19 Recovery
- 3 Ways To Improve Your Crisis Communications Plan After COVID-19
- Enhancing Decision Making With ERM
- Nation-State Hackers Reportedly Hunting For COVID-19 Research
- We Need Mission-Focused Risk Management Programs To Adapt To Changing Circumstances
- New Report: Risk Management in the AI Era: Navigating The Opportunities and Challenges Of AI Tools in the Public Sector
- Risk-Based Decision-Making: A Key Capacity for Government Today
- How To Leverage ERM Principles to Better Respond to COVID-19-Related Risks
- Eye of The Beholder: Understanding the Psychology of Risk Perception to Improve Risk Management
- Coronavirus News Being Used To Sneak Malware Past AV Programs
- Risk Management Lessons from Coronavirus
- On the Horizon: Six Emerging Priorities for Risk Professionals
- The Evolution of the Risk Manager
- Risk Management Salary Trends
- Mitigating Payment Fraud Risks
- DISA Breach Likely Exposed Personal Data On At Least 200k
- Risk Management for "Hacker-Less" Security Risks

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.

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:

- How can the agency ERM process and risk appetite principles be used to assist in mitigating strategic (long-term) risks resulting from COVID-19?
- What are some of the top challenges facing agencies in integrating the OMB A-123 ERM framework with strategic objectives and decision-making processes?
- What methods can agencies use to identify risks that are not already realized problems?
- How does the application of ERM differ in making risk mitigation decisions vs. routine decision making?

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


© 2019 Ernst & Young LLP. All rights reserved. ED None.
To prepare for the risks of tomorrow, you must disrupt today.
EY's Government & Public Sector Risk team is committed to building a better working world by helping our clients to confidently take and capitalize on risks as they shape the Federal agencies of the future. How can we help you make better data driven decisions and unlock organizational value?
Learn more at ey.com/govpublicsector
EY
Building a better working world

Thought Leadership

READ AT YOUR OWN RISK!

By George Fallon, Director, and Devin Borden, Manager, RMA Associates

Since the issuance of OMB's Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016), the Federal community, as a whole, has been looking for detailed guidance to help implement ERM. Now, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) has published a useful guide. Although there are several helpful resources, books, and articles published explaining the ERM process, the CIGIE issued a down-to-earth practical implementation guide: *Enterprise Risk Management Practitioner's Guide for Offices of Inspectors General* (October 2019) (Guide). The Guide provides a straightforward governance and management structure to implement risk management activities. Whether it is the Offices of Inspectors General (OIG) or program management, both are held accountable for their performance, compliance, and management of risk. The voluntary Guide is written specifically for the Inspector General community. However, its principles and techniques are not unique to OIGs and can be useful for the Federal community at large.

ERM Benefits

The objective of the Guide is to share good risk management practices and provide implementation activities to facilitate the adoption of ERM. As such, it is critical to appoint ERM champions and capture the agency's buy-in as the initial step.

The benefits of a good ERM program include:

- Improving mission delivery;
- Establishing a cohesive focus on stakeholders' expectations;
- Enhancing organizational culture;
- Heightening awareness about risks and risk management;
- Boosting engagement; and
- Increasing trust throughout the organization.

Implementation Tips

The Guide offers best practices for successful ERM implementation, such as the function must be appropriately placed within an agency and senior leadership must be involved in its support and execution. Also, ERM reporting lines and staffing levels must be well-defined. Equally as important, ERM staff should possess soft skills, be able to think strategically, and have functional knowledge of the agency.

The Guide notes it is very important to:

- Communicate ERM benefits in writing, most often in the organization's ERM framework;
- Develop and implement a risk assessment process that includes employee input, as well as management's perspective;
- Ensure transparency, both in terms of the process and the results, sharing plans and results, i.e., via email or internal ERM community web pages; and
- Demonstrate the full support of leadership by establishing a Risk Management Council (RMC) inclusive of top leadership, as well as identifying an ERM champion at the executive level.

The agency should establish an RMC charter identifying goals, responsibilities, and reporting lines. The RMC must include high ranking officials that influence or can make strategic decisions. Also, the RMC should actively support and commit to the agency's core values and enforce transparency and accountability by clearly communicating expectations for managing risks and establishing ERM practices and capabilities. Furthermore, the RMC should promote the core values of independence, integrity, respect, service, stewardship, transparency, and trust in all ERM activities.

Developing an ERM Framework

ERM must be carefully planned before implementation. The goal of the program is to control risk, so agency performance and compliance are free from material error and produce desired results. One size does not fit all. An agency's ERM implementation will vary depending on the strength of its risk management controls, budget, organizational culture, structure, and size. It is vital for the agency to outline a well-defined process to identify, assess, mitigate, and monitor control risk.

The framework may include:

- Developing a common risk language so all employees speak the same language when discussing and managing risks to ensure effective and quick communication across the organization;
- Developing an effective organizational structure that promotes the early identification, assessment, and management of key risks; and
- Creating a process that embeds risk management within all critical processes to ensure risks can be managed effectively.

In this stage, agencies develop risk categories in broad risk areas (e.g., strategic, environmental, operational, financial, informational) and group them within the risk areas to further categorize the risks. In addition, in this phase, the agency defines risk

attitude, risk management philosophy, risk appetite, risk tolerance, risk assessment, risk rating criteria, and other definitional attributes of the ERM program.

As in any effective program, the ERM program must be measured. The Guide introduces a useful scoring methodology for testing controls from a scale of 1 to 5:

1. Ineffective or Ad Hoc
2. Somewhat Ineffective
3. Effective
4. Very Effective
5. Extremely Effective

Implementing ERM

The effort in implementing an ERM program should not be underestimated. The implementation can often be troubled with difficulties, stress, surprises, and resistance. Note, an agency can leverage the work performed by other organizations to determine what will work for them while considering their own uniqueness. It is also beneficial to maintain a library of ERM material. Moreover, ERM planners should conduct focused and organized interviews so they are effective and collect the appropriate risks. After the interviews, the risks are identified, aggregated, analyzed, and assessed as an input to risk mitigation plans, making monitoring of risk mitigation plans essential for improving organizational capacity to address risks.

The Guide lists response options to risk, including:

- Assume - Acknowledge the existence of a risk and make a deliberate decision to accept it without engaging in special efforts to control it. Approval of management should be required.
- Avoid - Adjust requirements or constraints to eliminate the risk. This adjustment could be accommodated by a change in funding, schedule, or requirements. Choosing avoidance suggests the organization was not able to identify a response that would reduce the risk to an acceptable level of severity. Therefore, they do not undertake the action containing risk.
- Pursue - Seek an increased level of risk to enhance organizational performance. When choosing to pursue risk, management understands the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable risk tolerance.
- Reduce/Mitigate - Manage the risk by undertaking activities to lower or reduce the significance or likelihood of a given risk, such as establishing controls to mitigate the risk.
- Share/Transfer - Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk.

Integrating and Embedding ERM within Organizational Culture and Other Processes

Fraud risks can be integrated by leveraging a variety of existing processes. The Government Accountability Office (GAO), OMB, and Public Laws delineate fraud risk requirements that can be folded into the ERM program.

GAO's *Green Book* lists fraud risk factors including:

- Incentive/Pressure - Management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud.
- Opportunity - Circumstances exist, such as the absence of controls, ineffective controls, or the ability for management to override controls, which provides an opportunity to commit fraud.
- Attitude/Rationalization - Individuals involved can rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

Moreover, OMB A-123 was updated to require agencies to (1) use a risk-based approach to evaluate fraud risks and implement financial and administrative controls to mitigate such risks; (2) collect and analyze data to monitor fraud trends and improve fraud prevention controls; and (3) use the results of monitoring, evaluations, audits, and investigations to improve fraud prevention, detection, and response.

The *Fraud Reduction and Data Analytics Act of 2015* (Public Law 114-186, June 30, 2016) (FRDAA), created expectations for agencies to establish financial and administrative controls for managing fraud risks. Agencies can also leverage quality assurance reviews to identify risks and enhance internal controls within their business processes.

Sustaining ERM

ERM requires constant attention and adjustment to maintain the program. The process of sustaining ERM may be different for every organization. However, executive management's consistent support for the RMC and ongoing risk training to keep the practitioners up-to-date with current techniques is a MUST! Agencies should also encourage employees to earn an ERM certificate and consider subscribing to services and outside vendors to help maintain and grow their ERM capabilities.

Finally, continuous monitoring and assessment of risk are vital. Agencies should measure their maturity level to ensure they manage risk on a consistent and sustainable basis and promote risk culture in their values, beliefs, knowledge, and attitudes, so they may control what otherwise may be a CATASTROPHIC event. Stay safe my fellow practitioners and beware! Risk is all around but go forward without fear as it can be tamed with ERM.

In brief, *The Enterprise Risk Management Practitioner's Guide for Offices of Inspectors* is a useful tool, not only to the OIG community but also for all Federal agencies.

George Fallon may be contacted at g.fallon@rmafed.com, and Devin Borden may be contacted at d.borden@rmafed.com.

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	Contact
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
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
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	Valerie Lubrano, Chair, vlubrano@gmail.com or aferm.sacop@gmail.com

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.

Thought Leadership

Expoiting technology for ERM

By Marshall Toburen, Risk Management Strategist, and Dan Carayiannis, Public Sector Director, RSA

The Case for ERM Technology

It has been almost four (4) years since the revision of the OMB's Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. One thing ERM teams have learned over this time is ERM is no small undertaking. Documenting and understanding mission and objectives, risks to mission and objectives, fraud risks, outsourced risks, controls, control assurance and testing, and reporting can be an overwhelming amount of work. The problem is compounded by the fact that little, if any, of the ERM domain is static. Objectives, risks, and controls change all the time. Some changes accompany changes within the organization, staff, and technologies, while many others are associated with third-party service organizations or result from changes in vulnerabilities and external threats. Many changes cannot be easily anticipated, yet agencies are charged with effectively responding with alacrity when surprises arise.

Government organizations today face a rapidly changing regulatory and agency risk landscape and will likely continue to do so in the years to come. Their ERM strategies may not be positioned to adapt to these changes. Decentralized organizational structures, multiple tools, and various processes and systems make it difficult to see a clear and consistent risk picture across the organization. Additionally, the number, complexity, and velocity of risks are increasing, and the speed at which these risks emerge means organizations have less time to effectively respond.

The current COVID-19 global healthcare crisis provides an illustration of how an environmental risk can significantly impact the processes and functions a government organization is charged with providing. Agencies initially struggled to provide the services other dependent organizations and the general public rely on and require, and to ensure employee safety at the same time. The well-documented cyber breach at the U.S. Office of Personnel Management (OPM), with its corresponding identity risk and financial cost ramifications, provides another illustration of the unfortunate consequences of unanticipated and unaddressed risk.

Most risk management teams are managing different types of risk—cyber, third-party, personal, financial, policy, safety, environmental, public-service, and others, all typically in different silos—and assessing them using separate methodologies and measurements. Such an ad hoc risk management approach is likely overloading resources and isn't providing a consistent, real-time, aggregated view of risk across the

business to leadership teams. Without this visibility, risk cannot be consistently managed within the organization's risk appetite.

Organizations are finding that existing risk and audit approaches, process, expertise and tools are not sufficient to deal with a dynamic and ever-evolving risk landscape. In addition, fewer resources and added responsibilities within risk and audit teams argue in favor of an approach that is more flexible, adaptive and transformational. Dynamic risk planning should be incorporated into approaches and results, driving risk and audit organizations to work more closely together. The executive team needs assurance that the organization's internal control framework is adequately designed and operating to ensure that risk is being effectively managed, so that agency leaders have the confidence and complete understanding of the organization's risk profile they need to make sound risk-based decisions.

Operationalizing ERM Programs with Technology

Effective ERM is synonymous with good governance, but good governance cannot be achieved without "operationalizing" ERM. Operationalization is necessary because enterprise risk is dynamic and quite voluminous, requiring the engagement of too many stakeholders to be done with available resources. Consider the method most organizations employ to capture objectives, risks, and controls. Most organizations start out creating custom campaigns with Microsoft Excel templates that they email to dozens or more managers, asking them to fill in the blanks—even while realizing that a good number of the managers will interpret the request in different ways, won't be familiar with the terminology, and may not know how to assess a risk or write an internal control statement. Worst-case scenario, many managers will not respond on time, if at all. As a result, risk teams are caught up in an endless cycle of looking for response gaps and vetting the adequacy of responses received.

With risk management technology today, there is no reason to commit valuable resources to chasing down responses from managers. Here are examples of how integrated risk management solutions can operationalize ERM, saving resources and money, improving completeness and accuracy, and enhancing governance:

1. Automated workflow can distribute objectives, risks and controls collected in the last cycle to the current owners for rewording (if appropriate), reaffirmation and reassessment. If there are no records for a manager to review, a blank form can be distributed for managers to declare their objectives, processes, supporting objectives, key risks and key risk-mitigating controls. Terminology and assessment techniques can be explained with embedded help text, and blank fields can be minimized by requiring all fields be completed before the record can be submitted.

   The risk management team has real-time graphic visibility into the status of management's response: how far, from 1-100%, are managers from being

complete? Risk teams can proactively reach out to managers that seem to be struggling. Workflow can send management reminders and automatically escalate past-due responses up the management chain. Risk teams no longer need to send and re-send emails imploring managers to participate.

2. ERM technology today can be structured to capture information for regular refreshes of risk and control registers and risk assessments. Most ERM teams today endeavor to have management do these refreshes on at least an annual basis. Some publicly traded private sector organizations even expect them to be done on a quarterly basis! ERM technology today can also be structured not just to capture these refreshes, but also to report all new and changed objectives, risks and controls, and associated risk assessments, to the ERM team for review and approval before being updated to the system of record. As a result, ERM teams no longer must look at every response but only those that change, and they play the pivotal role to make sure anything that goes into the system of record makes sense and conforms to approved taxonomy, sentence conventions and assessment approaches. Continuous monitoring of changes coming in from management across the organization gives the ERM team near real-time visibility into changes in the organization's risk profile. They may choose to engage in helping managers with their new risk profile or simply report significant changes up to the organization's governance teams.
3. ERM technology can help with the increasing challenges outsourced services pose to organizations. Third-party risk is often opaque, and risk assessments require the engagement of many stakeholders (legal, insurance risk transfer, information security, compliance and business resiliency). With an ever-increasing government dependency on third-party contractors and technology organizations (and consequently, an expanded risk "footprint"), an integrated risk management technology today can standardize the process of collecting the inventory of third parties, documenting who "owns" the relationship, and understanding the purpose of the relationship and how significant it is to the organization. Automated workflow can be utilized to solicit internal control questionnaires from third parties, and assess legal contracts, insurance certificates and risk assessments. Go/no-go decisions can be programmatically enforced consistent with the organization's risk appetite and tolerance.
4. Reporting is dramatically simplified using integrated risk management technology. Managers granted access can see an online, real-time profile of risk within their domain of responsibility. Control gaps identified through assertions, or management or audit testing can automatically open issues that are tracked from origination to disposition within the accountable management chain. Periodic reporting, regardless of the cycle (weekly, monthly, quarterly, etc.) is easily produced, including top risks, key controls, objectives most at risk, vendors to watch, risk profile of most important vendors, outstanding issues by criticality and

due date, new policies and policies to be reaffirmed, and policy exceptions and exceptions to be reaffirmed.

These are just a few examples of possible ways ERM technology can be exploited to save management and ERM teams time and money while improving the organization's ERM capabilities.

Stay tuned for our next thought leadership contribution: *Evaluating ERM Technology and Finding the Right Fit for Your Organization.*

Marshall Toburen may be contacted at Marshall.Toburen@rsa.com, and **Dan Carayiannis** may be contacted at Dan.Carayiannis@rsa.com.

AFERM Officers, Committees, and Communities

Officers

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

Audit
Alex Ng

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

Planning
Christina Girardi, Chair
Marc Pratta, Co-chair

Programs
Varun Malhotra, Chair

RIMS Liaison
Cynthia Vitters

Summit 2020 Committee
Meredith Stein, Chair
Marianne Roth, Co-chair

Volunteers
Irena Marchand, Chair
Janice Ho, Co-chair

Cyber ERM Community of Interest
Nahla Ivy, Chair

Data Analytics Community of Practice
Curtis McNeil, Chair

Small Agency Community of Practice
Valerie Lubrano, Chair

Corporate Advisory Group (CAG)
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
Gold Sponsors
Bobbie-Jo Pankaj, Grant Thornton
Silver Sponsors
Jeannine Rogers, AOC Solutions
Bert Nuehring, Crowe LLP
Maurice Guloy, Galvanize
Tim Mobley, IRIS Intelligence
Paul Marshall, MIL Corp
Wendy Morris, MorganFranklin Consulting
Shawn O'Rourke, Pro-Concepts
George Fallon, RMA Associates, LLC
Carrie Everett-Vaughan, RSA
Sim Segal, SimErgy Consulting
Robert Crawson, Sword Active Risk
Tashu Trivedi, TFC Consulting, Inc.
Paul Marshall, The MIL Corp
Celine Serrano, WAEPA
Jay Colavita, Workiva/Vertosoft

CAG Liaison
Souyma Chakraverty, Chair

RIMS-CRMP-FED Certification

Corporate Sponsors

Thank you for your support!

Platinum Sponsors

11TH HOUR SERVICE

Deloitte.

EY Building a better working world

Guidehouse

KEARNEY& COMPANY

KPMG

Gold Sponsors

Grant Thornton

Silver Sponsors

ARM Active Risk Manager

AOC SOLUTIONS

Crowe

GW

IRIS INTELLIGENCE

MIL corp.

Educational Development and Community Partners