AFERM
Association for Federal Enterprise Risk Management

AFERM Updates

Issue 28
February 2019

Thought Leadership for the Federal Enterprise Risk Management Community

Contents

Highlights

This is the 28th issue of the quarterly AFERM Newsletter! It includes thought leadership articles from ERM practitioners with Grant Thornton, the IBM Center for the Business of Government, and Morgan Franklin.

AFERM Association for Federal Enterprise Risk Management

AFERM
Association for Federal Enterprise Risk Management

AFERM Updates

Issue 28
February 2019

Thought Leadership for the Federal Enterprise Risk Management Community

A Note from AFERM's President

2019 AFERM President Tom Brandt

ERM and Recovering from the Partial Government Shutdown

By Tom Brandt

As I write this message, a quarter of the federal government is recovering from the partial shutdown, with another deadline looming on the horizon for Congress and the President to reach a resolution for keeping government operations running through the rest of the fiscal year. While the prospect of a lapse in appropriations is a risk most agencies have identified and are required to plan for, the chance one would occur lasting more than 30 days was not considered to be of high likelihood. Yet this low-likelihood event did occur, and, as we all saw, the impacts were widespread, worsened over time, and are still now being identified and assessed.

I hope that the risk community was called upon to help agencies respond to and recover from the shutdown, although, in discussions with colleagues and peers, it seems there was a high degree of variability in the extent to which that has occurred. That means there may be an opportunity for risk professionals across the federal government to offer assistance in identifying and assessing shutdown related risks that may have or could still manifest and threaten the delivery of mission objectives. We can work with business lines to determine response strategies, and, as importantly, explore ways to partner with our business continuity and lapse planning teams to determine how to enable greater resiliency in the event of future disruptions to our operations.

It's also possible, given several bills that have been introduced in Congress, that the threat of future shutdowns or lapses may be eliminated via legislation that would, for example, keep agencies open and operating at prior year funding levels. While such laws would eliminate one type of risk, they could create new ones, especially alternative bills that would impose escalating reductions to agency budgets the longer operations continued without the adoption of new appropriations. AFERM will stay attuned to developments in this area and provide forums for discussion at future events as appropriate.

Due to the shutdown, we were unable to host Don Kettl for a discussion of his research and report on "Lessons for Improving Government Management from GAO's High Risk List", but thanks to Paul Marshall, we have a Risk Chat with Professor Kettl available on the AFERM web site. Take a listen to hear about actions agencies can take to get off (or stay off) the High Risk List, but also to hear how being on the List can help agencies manage and mitigate significant, long-standing risks.

If you weren't a member of the inaugural class that earned the RIMS-CRMP-FED credential in 2018, we hope you'll consider pursuing the credential this year. Through our continued partnership with RIMS, AFERM members can complete the prep course and take the test at a reduced rate. See our web page for further details and dates.

Planning is already underway for the 2019 AFERM Summit. As all-volunteer organization, we actively encourage your continued support and ideas for programs and events, and we welcome additional volunteers to help with the Summit – contact aferm.volunteers@gmail.com to learn how you can help.

Tom Brandt, AFERM President, may be contacted at president@aferm.org.

ERM Events

AFERM hosts a networking event, including a discussion on ERM and the partial government shutdown

On February 13, 2019, AFERM hosted an event featuring a penal discussion related to the takeaways and implications from the recent partial government shutdown in the context of enterprise risk management (ERM). The discussion was facilitated by Tom Brandt and included a panel comprised of Karen Hardy, Alice Miller and Doug Webster (pictured below).

The audience was actively engaged and offered numerous comments and questions. The panel discussion was followed by a networking session with refreshments. Below are a few highlights from the panel discussion.

The importance of ERM and risk management

The panelists discussed how the recent partial government shutdown emphasized the importance of ERM and effective risk management practices. One panelist noted that it can sometimes be difficult for people to visualize a risk event in order to understand the importance of risk management. Although unwanted, the partial government shutdown provides a tangible example of a significant risk event. This highlights the need for agencies to be aware of and prepared for different types of potential risks events. This includes preparing not just for another shutdown, but also for different types of potential future disruptions to operations. One panelist

pointed out that while internal controls often focus on managing the risks of today, risk management is much broader than that and must also take into consideration potential risks of the future.

Strategic decision making in Light of the Shutdown

The panel talked about the need to make strategic decisions and tradeoffs in light of the shutdown, and that these should be made in the context of risk appetite. The panelists noted that agencies may be willing to take on more risk in certain areas now than they would have before the shutdown. One panelist also noted that the shutdown could lead to the government and individual agencies having to rethink overall what they are trying to accomplish, including potentially modifying goals and targets.

Upcoming events of interest to ERM practitioners

Following is a list of events upcoming that may be of interest to ERM practitioners. Please visit our website for more information at https://www.aferm.org/events-list/.

- March 14, 2019 - AFERM Luncheon with Presentation by Kate Kelley, Superintendent of Arlington National Cemetery
- March 20, 2019 - Insight Exchange Network (IEN): The Government Anti-Fraud Summit
- March 21, 2019 - Public Sector Network: Women Leaders in Public Sector with Georgetown University
- April 11, 2019 - AFERM & AGA ERM Workshop: Driving Organizational Value - Enhancing Performance
- May 29, 2019 - ASMC Professional Development Institute
- June 17, 2019 - SimErgy: 9th Annual ERM Boot Camp
- July 21, 2019 - AGA 2019 Professional Development Training
- October 29-30, 2019 - AFERM 2019 Summit
- November 4, 2019 - RIMS ERM 2019 Conference

Thomas Holland of Guidehouse coordinates the AFERM luncheons, networking, and other events. He may be reached at AFERM.Lunches@gmail.com.

AFERM Association for Federal Enterprise Risk Management

AFERM Updates

Issue 28
February 2019

Thought Leadership for the Federal Enterprise Risk Management Community

Thought Leadership

Tips for Better Enterprise Risk Management

By Darius Hinton

Risk is, well, risky—but your organization can't grow without it. The key is that risk needs to enable organizational strategies and culture. Unfortunately, strategy development and enterprise risk management (ERM) often compete for relevance within organizations. Strategy is usually a risk-seeking activity, while ERM seeks to identify and mitigate the very risks a strategy creates. Some common issues in integrating strategy and risk management include duplicating risk management and strategy development process efforts; competing objectives between the risk management plan and program strategy; and lack of resources for maintaining a risk management program.

In setting and executing strategy, organizations inherently accept risks. Therefore, it makes sense for ERM strategy to be developed alongside and inside the strategic planning cycle. Few companies, however, do so. A 2016 report from the North Carolina State ERM Institute concluded that only 25% of organizations integrate ERM into strategic planning. With key decision makers and stakeholders already engaged in identifying the vision for the organization, there is an opportunity to identify factors that could hamper strategy execution.

After identifying external risks, many organizations perform an internal analysis to identify competitive or strategic advantages. The internal analysis is completed using one or more of the following frameworks: strengths, weaknesses, opportunities, and threats (SWOT), Porter's Five Forces, or the 3Cs Model. This output is critical during the risk assessment and identification phase. For example, weaknesses and threats identified in a SWOT analysis may be used as indirect and direct starting points in risk identification. "Opportunities" are uncertainties with a potentially positive outcome (or positive risks).

At this point, organizations should ask a number of questions. What events would change the positive outcomes of uncertainties to negative? How would opportunities become risks? What happens if we don't take advantage of these opportunities? The answers to these questions are risks to long-term strategy. After assessing the impact of these risks, stakeholders should begin contemplating mitigation strategies, so they may be fully integrated into the overall strategy. This prevents an organization from pursuing competing objectives or duplicating efforts in risk assessment and promotes a risk-conscious organization. This also allows leadership to develop and communicate the strategy in risk terms to the organization.

Categorizing risks allows strategic thinkers to easily identify patterns and trends. However, strategy and risk management have too many interconnectivities and are too

complex to rely on simple classification. Despite agreement with this premise, many organizations compartmentalize risk and then assign it based on simple categories.

For example, organizations may categorize risks as supplier-related, technological, operational, external, etc. More often than not, the focus in categorization is compliance-based and does not consider inherent strategic and enterprise-wide risks, which ERM is designed to address. It also fails to acknowledge that risks do not materialize in a vacuum. For example, a supplier-related risk and information technology (IT) risk materialized and an information control is compromised in the supply-chain process. This in turn causes quality control issues, and now a quality risk has materialized. This quality risk can lead to an external risk if it affects customer perception of the product.

All of these risks decrease progress towards a strategic objective. This slippery slope is hard to stop, and because risks were assigned to functional area leads (based on their category), operational leads may be inclined to blame rather than collaborate to mitigate problems. If the IT team is concerned only with mitigating information risks and the quality team is focused on supplier quality, neither team has been encouraged to work together in addressing the impact IT risk triggers, which then cascades down and across the organization.

To address this issue, there are two steps an organization can take. One is to rethink how risks are categorized, and the other is to assign risk mitigation to the level where strategy is operationalized. Relabeling risks based on broader, strategy-based dimensions may promote a more collaborative view of risk mitigation. A 2012 Harvard Business Review article written by Robert Kaplan and Anette Mikes recommends classifying risks as preventable (risks with no strategic benefit such as fraud or failures); strategic (risks accepted in achieving objectives such as researching new product offerings); or external (uncontrollable risks from the environment like macroeconomic trends).

Expanding on Kaplan's and Mikes' framework for risk classification, risks can be and often are interconnected between the three dimensions. External risks place pressure on strategic risks, which influence potential realization of preventable risks. This may also work from the bottom up: A preventable risk may inhibit strategic objectives, influencing the strategic risk level, and in turn, external risks are affected, as is the case in the supply chain example. During the risk assessment, data collected should identify other associated, second-order risks and potentially affected strategic objectives if the risks materialize. Once these risk relationships are identified, the next step is assignment and monitoring.

The assignment of risk monitoring and mitigation is an indication of the priority organizations give to risk management. Strategic objectives should be assigned to a level where decision-making can most affect the direction of operations towards achieving strategic objectives. This allows policies and tactics to be approved and

implemented effectively. Risk mitigation should be assigned at the same level. Assigning risk management responsibilities to strategic decision makers aligns strategy and risk management. With the authority to make tradeoff decisions between the occurrence of a risk event and its related strategic objective, the decision maker can decide which response would most likely to be adhered to. Assigning mitigation to a lower, more tactical level increases the probability that risk management will compete with strategy and can lead to confusion across operations.

Risk monitoring should be a part of an organization's internal strategic reporting to ensure risks are monitored alongside strategy. These metrics can be embedded in the areas that track success towards accomplishing objectives, so separate reporting areas are often not required. For example, a government IT division responsible for maintaining communication systems can integrate metrics to track vulnerabilities to core communication systems. Another example would be a scorecard that tracks attempted breaches to a customer-facing support solution. Many metrics already inherently incorporate different types of risk control measures. These types of metrics should be highlighted at the decision-maker level; the risk details can be tracked separately, but the key is to keep risk management closely aligned with strategy through reporting.

ERM should not be considered an additional process to be completed by leadership. It is a process enveloped in the development of strategy. Every strategic decision should consider the uncontrollable factors that might affect those decisions, the uncertain factors resulting from the decisions and the capabilities required to enact them. This is what risk management is truly about. Continuing to treat risk management as a separate process limits the full evaluation of strategy, leading to inadequate strategy development and a risk-nescient plan. Choosing to keep strategy and risk management processes separate, with separate responsibility for strategy execution and risk management, reduces an organization's ability to respond quickly and effectively when risks materialize. Keeping the processes separate also increases time spent on duplicative efforts and can create competing objectives. Leaders should evaluate how risk management is developed in their organizations and look for ways to integrate it into the strategic development cycle wherever it does not exist.

Darius Hinton, MorganFranklin Consulting, is on a military detail. View more thought leadership from MorganFranklin Consulting on ERM and other government topics at https://www.morganfranklin.com/category/insights/government-insight/

AFERM Association for Federal Enterprise Risk Management

AFERM Updates

Issue 28
February 2019

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM Summit 2018

Looking back at another successful Summit

The 2018 AFERM Summit was a tremendous success. Government and Private sector ERM Practitioners gathered for the multi-day conference to share insights, best practices, and a growing network of connections. AFERM's Communications Committee spoke with 2018 Summit Chair Sean Vineyard about last year's event and his experience and insights.

This past year, the speed at which registration occurred served as an early indicator of the continued and growing interest in the event. The Summit attracted more than 400 registered participants and dozens of volunteers, 70% of whom were federal risk practitioners. Just six-seven years ago, the Summit was able to be held in the auditoriums at George Mason University. Now, that pioneering group of 160 participants has almost tripled in size. Sean described the high point of his experience organizing the summit: "The best moment of this journey was during a closing general session on the first day of the Summit. I walked into the atrium and saw hundreds and hundreds of engaged people, smiling and clapping." The high level of energy and enthusiasm continued through the rest of the event and later translated into high marks from Summit participants in their responses to a survey asking about their satisfaction with the event organization, sessions, and venue.

The 2018 Summit team secured the Ronald Reagan Building and International Trade Center for three (3) years. The facility offers the adequate space for continued growth of the Summit and can comfortably fit a thousand participants. The 2019 Summit team will have a head start on creating another fantastic event with the venue already secured this year's event.

Time becomes a precious commodity when organizing such complex and multifaceted events. When asked what advice he would give to the 2019 AFERM Summit co-chairs, Nicole Puri and Meredith Stein, Sean could not emphasize enough the importance of beginning preparations as early as possible. Last year, Sean said the team began holding initial planning meetings just a few weeks after the 2017 Summit concluded. He also noted that ample preparation time should be paired with flexibility. As all the speakers volunteer their time and expertise, consideration must be made to account for the last minute changes in schedules, travel, and so on. "When planning the risk management Summit with a group of risk managers, we were definitely prepared with a Plan B, C, and D," Sean said.

The Summit's success would not be possible without volunteers. The AFERM Summit is a unique community 100% driven by the will and enthusiasm of volunteers who contribute their time and energy. A great team of volunteers who are passionate about ERM in the federal sector really drive the success of this two-day event. During the preparation for the 2018 Summit, more than 45 volunteers in different roles and at

different times helped to plan and execute the event. The core planning team consisted of five subcommittees each with a chair and a co-chair, and the members of the AFERM Board were heavily involved on a weekly and sometimes even daily basis.

As federal ERM professionals and AFERM Community members, we thank Sean Vineyard and his dedicated Summit team for a job well done! We are already excited for the opportunity to gather together and learn from one another at the 2019 AFERM Summit.

Sean Vineyard, Managing Director, 11th Hour Consulting, may be reached at svineyard@11thhourservice.net.

AFERM Awards and Recognition

Celebrating the success of AFERM members

Annually, through the ERM Awards Program sponsored by Deloitte, AFERM recognizes risk management professionals who make lasting impacts on Federal organizations. Awardees are nominated by other risk management professionals, and at this year's AFERM Summit in October 2018, we were pleased to recognize the following persons.

ERM Leaders of the Year:

- **Sherri Berger**, Centers for Disease Control and Prevention
- **Christine Jones**, U.S. Department of Health and Human Services

This award honors leaders in the Federal sector who have demonstrated outstanding and sustained leadership and made exceptional contributions to the practice of ERM in the Federal sector.

ERM Professional of the Year:

- **Mai Shintani**, Federal Insurance and Mitigation Administration

This award honors Federal professionals who have demonstrated exceptional initiative, professional development, achievement, and leadership early in their careers.

ERM Hall of Fame:

- **Tom Stanton**, National Academy of Public Administration and former SES at the Federal Trade Commission

This award honors Federal professionals that make extraordinary contributions to advancing the ERM discipline in the Federal sector.

ERM Volunteer of the Year:

- Sheri Francis, Special Inspector General for Afghanistan Reconstruction

This award honors federal professionals committed to the advancement of ERM in 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.

From Left: Peggy Sherry, Tom Stanton, Christine Jones, Sheri Francis, and Tom Brandt. On Right: Mai Shintani.

Not Pictured: Sherri Berger.

Congratulations to our 2018 AFERM ERM Award recipients! We thank you for your dedication to the Federal ERM profession!

If you wish to nominate an outstanding Federal ERM professional for a 2019 award, please download a nomination form from our website at https://www.aferm.org/awards/. Nominations should be submitted via email to AFERM.Awards@gmail.com.

AFERM
Association for Federal Enterprise Risk Management

AFERM Updates

Issue 28
February 2019

Thought Leadership for the Federal Enterprise Risk Management Community

ERM Resources

AFERM's podcasts continue the ERM dialogue

Are you a fan of podcasts? Check out AFERM's ERM podcasts on our website. Paul Marshall and Tal Seaman discuss ERM with Chief Risk Officers and risk management professionals. Here's the line-up:

- Episode 1 – Tom Brandt, Internal Revenue Service
- Episode 2 – Wendell Conner, Housing and Urban Development, Public and Indian Housing
- Episode 3 – Todd Grams and Cynthia Vitters of Deloitte on the RIMS-CRMP-Fed Micro-Credential
- Episode 4 – Craig Bennett, U.S. Coast Guard
- Episode 5 – Nicole Puri, Pension Benefit Guaranty Corporation
- Episode 6 – Meredith Stein, National Institutes of Health
- Episode 7 – Jacki Ponti-Lazaruk, USDA Rural Development
- Episode 8 – Lori GIblin, the Corporation for National and Community Service
- Episode 9 – Jason Leecost, Ginnie Mae
- Episode 10 – Jennifer Hills, King County, Washington
- Episode 11 – Don Kettl, author of Managing Risk, Improving Results: Lessons for Improving Government Management from GAO's High-Risk List

---

Paul Marshall, Vice President, MILCorp, may be reached at pmarshall@milcorp.com, aaand **Tal Seaman**, Owner and CEO, Navigator Solutions, may be reached at tseaman@navigatorsol.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:

- Predicting Risk Management Challenges in 2019
- Washington Metropolitan Area Transit Authority: Actions Needed to Strengthen Capital Planning and Track Preventive Maintenance Program
- The Changing Risk and Liability Landscape for IT Security and Data Risks
- Climate Change: Activities of Selected Agencies to Address Potential Impact on Global Migration
- Six Tips For Risk Managers When Assessing Automation Hazards
- Looking Ahead: The 2019 Risk Landscape
- The Use of Entity Analytics in Financial Crimes Risk Management
- Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management
- Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions
- Improper Payments: Additional Guidance Needed to Improve Oversight of Agencies with Noncompliant Programs
- PBGC's Fiscal Year 2018 Purchase Card Risk Assessment
- Fraud Risk Management: OMB Should Improve Guidelines and Working-Group Efforts to Support Agencies' Implementation of the Fraud Reduction and Data Analytics Act
- Engaging Employees in Their Own Duty of Care
- Mitigating Third Party Risk in Supply Chains
- Using Actuarial Reports to Help Manage Risk
- Using Adaptive Behavioral Analytics to Detect Fraud
- An Enterprise Approach to Data Security
- Investing in Workplace Safety

To view the newsfeed, visit "Resources" on the AFERM website and choose "Newsfeed" or use the following link: https://www.aferm.org/erm-newsfeed/. The "Resources" page provides multiple ways to sort the large library of content by audience, content type, and resource or choose "View All Resources" to scroll the full library.

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

AFERM Association for Federal Enterprise Risk Management

AFERM Updates

Issue 28
February 2019

Thought Leadership for the Federal Enterprise Risk Management Community

Thought Leadership

Do You Really Know Your Fraud Risks?

By Linda Miller, Grant Thornton Public Sector Fraud Risk Mitigation Leader and Denise Lippuner, Grant Thornton Public Sector Risk Advisory Services Leader

An Enterprise Risk Management (ERM) program should consider all risks to an organization. One risk that is often dismissed is fraud.

Fraud has well-known financial and reputational ramifications. But if your organization is like many others, "It can't happen here" is a pervasive belief. When this belief is held by leadership, there is very little chance that risk management will be taken seriously. Significant fraud avoidance and mitigation are built on top-level awareness and commitment, and effective assessment to direct risk management activities. Ignoring the potential for fraud is expensive. According to the *Report to the Nations*, released in 2016 by the Association of Certified Fraud Examiners (ACFE), a typical organization loses 5% of its annual revenues to fraud. Losses can mount much higher.

While the Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (A-123), requires agencies to evaluate fraud risks as part of an agency's risk profile, many agencies merely scratch the surface when it comes to truly assessing their fraud risk exposure and very few have established programs around fraud management.

The five phases of fraud management:

1. Establish governance with top-level anti-fraud commitment
2. Create a formal fraud risk assessment process
3. Develop control activities aimed at the highest fraud risk areas
4. Implement fraud reporting and investigation procedures
5. Ensure oversight and monitoring of internal controls and new schemes

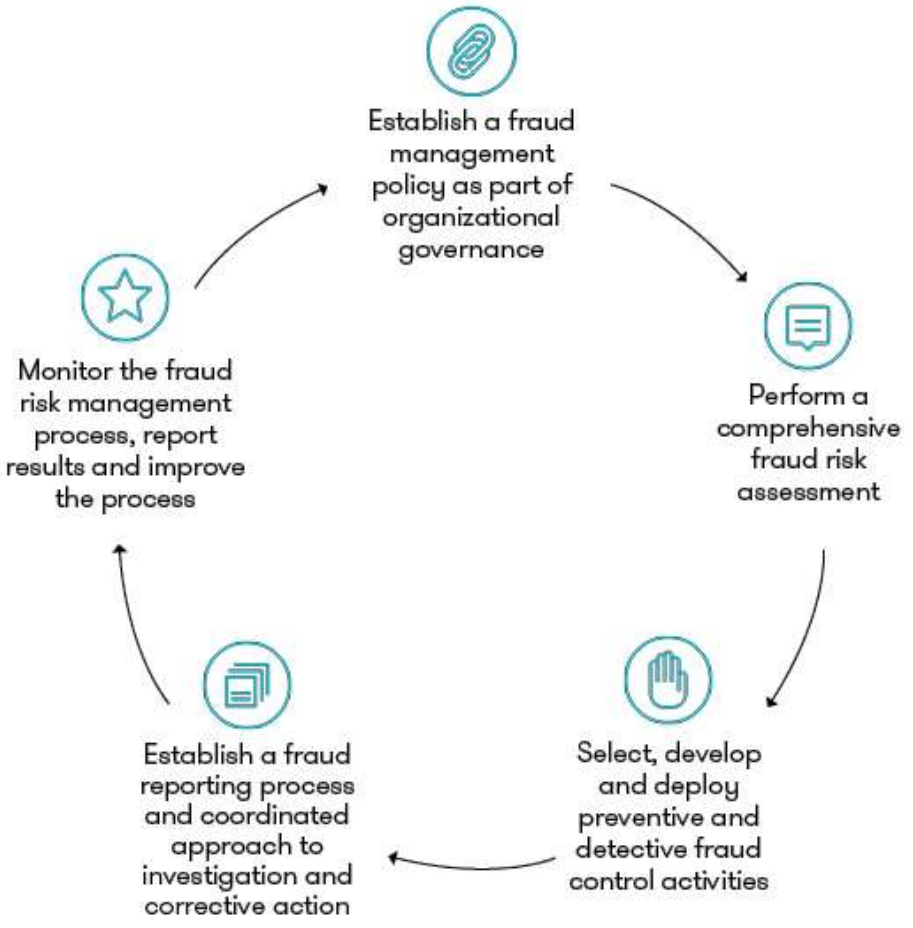
Commit to fraud risk management from the top

While it's easy to acknowledge that fraud prevention is the most cost-effective approach, proactivity isn't always on the agenda. Too often awareness comes as a hard lesson. Avert such lessons by raising awareness to the level of a C-suite priority.

C-suite executives get ahead of issues by charging senior executives with fraud risk management responsibilities. This commitment is the first of the five phases of a

productive fraud risk management program. Direction for all the phases can be found in the *Fraud Risk Management Guide*, issued jointly in 2016 by the Association of Certified Fraud Examiners (ACFE) and the Committee of Sponsoring Organizations of the Treadway Commission (COSO). A similar approach to anti-fraud programming is described in *Framework for Managing Fraud Risks in Federal Programs*, the U.S. Government Accountability Office guide issued in July 2015. Most recently, the Antifraud Playbook was issued in October 2018 by the Chief Financial Officers Council (CFOC) and the U.S. Department of the Treasury, Bureau of the Fiscal Service. This playbook provides practical guidance, leading practices, and helpful resources for agencies to establish or enhance their anti-fraud programs.

Ongoing, comprehensive fraud risk management framework



Source: Association of Certified Fraud Examiners and the Committee of Sponsoring Organizations of the Treadway Commission

The overarching phase — second only to commitment — is a comprehensive, enterprise-level fraud risk assessment.

Assess your fraud risk exposure, current and future

Your staff and stakeholders, who know the day-to-day workings of the organization, are the best sources for a realistic fraud risk assessment. Structure a process to capture their on-the-ground experiences, perceptions and risk fears.

At the start of the assessment process, describe common fraud scenarios to which your organization might be vulnerable. Write fraud risk questions to determine the likelihood of the scenarios becoming reality, as well as impacts that could be anticipated. Then launch the collection procedure.

The initial fraud risk assessment is a baseline. Incorporate subsequent assessments to continuously raise awareness of and commitment to management of fraud in its many forms.

Help staff and stakeholders buy into assessments

Explain assessment as a collaboration to identify and mitigate vulnerabilities. Make fraud risk a comfortable subject to discuss. When “risk” is not a menacing word, stakeholders are more inclined to consider the possibilities of fraud. They’re also more likely to provide honest feedback if they feel safe from accusations when pointing out weak or missing controls.

Reduce trepidation through survey questions that minimize room for negative interpretation. Ask process-specific rather than personal-responsibility questions. Instead of “How effectively do you verify self-reported information?” ask, “Do you verify self-reported information in applications? If so, how many databases do you check? Do you use internal or third-party data? Have there been reliability concerns with verification data?” Responses will be more reliable because respondents will be more comfortable responding to process-specific questions.

Reliability will also hinge on the clarity of questions. Asking about risk likelihood and impact on a five-point scale will yield only a number from 1 to 5. For example, a question might ask for ranking exposure of personally identifiable information. Some respondents might interpret the risk as large-scale cyberattacks and some as printouts mistakenly left on a desk. The two events are very different. A better approach is to pose narrow, standardized questions. You could ask about the strength of controls to protect potential entry points, e.g., product types and channels. Answers can be converted into a rubric, with a quantitative risk score for each function. Results will identify the most crucial risk areas.

Facilitate fraud risk workshops

Address crucial risk areas with regular anti-fraud training. Keep in mind that people often assume best intentions. This tendency can skew the ability to make unbiased judgments. To nurture a fraud risk–aware culture, encourage healthy skepticism. Make sure that every training session promotes critical thinking and reports on internal or external events of any size.

A practical component of training is a schedule of facilitated workshops. In your workshops, assign participants the role of fraudster and prompt them to describe how they might perpetrate schemes. Allow time for open discussion of questionable activities and other possible warning signs. Note detected and emerging threats for updating your fraud scenario library.

Success is iterative

See the first fraud risk assessment as a baseline and include lessons learned in the next assessment. Fraud risk assessment is more art than science and will be more effective at some organizations than others.

Effectively managing your organization's fraud risk can be a long process. In the beginning, any assessment is better than none. Build a fraud scenario library, initiate anti-fraud training to enhance the organizational buy-in and design a structured survey to collect information from staff and stakeholders within your organization. Once you've established a baseline, subsequent steps will help your organization raise awareness about fraud lurking in the shadows.

Linda Miller, Director, Grant Thornton, may be reached at linda.miller@us.gt.com, and **Denise Lippuner**, Partner, Grant Thornton may be reached at denise.lippuner@us.gt.com.

AFERM
Association for Federal Enterprise Risk Management

AFERM Updates

Issue 28
February 2019

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM's Ask the Experts

ERM Resources for Federal Practitioners

AFERM recently deployed a resource accessible via the AFERM website – "Ask the Experts." This blog provides ERM practitioner's access to ERM experts and facilitates the exchange of ideas.

Here are some recent questions answered:

- What are some methods/strategires for promoting a healthy risk culture across the agency?
- What are some techniquest to leverage ERM information for the strategic objective review (SOR) process?
- Whouls agencies automatically focus resources on risks with the highest levels of residual risk, or should mor energy be placed in those that may exceed established risk tolerances (regardless of residual risk level)?
- Of those ERM programs that have a formal communications program, what does it look like?
- How do you consider existing cotrols in establishing the likelihood of the risk? Are risk responses by default internal controls?
- What are some effective methods to report the status and/or results of ERM activities to management?
- How long does it take to implement a fully compliant ERM program?

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

AFERM Association for Federal Enterprise Risk Management

AFERM Updates

Issue 28
February 2019

Thought Leadership for the Federal Enterprise Risk Management Community

Thought Leadership

An Overview of Potential Risks and Benefits of Using Artificial Intelligence in Government

By John Kamensky

Popular media and science fiction have posed scary scenarios for the future as a result of advances in artificial intelligence (AI); but what is a more realistic assessment, especially in the near-term? Furthermore, how can risks be assessed in more measured terms than seen in the movies, especially in government agencies and programs?

Advocates of AI promise great benefits – cheaper and more citizen-oriented services, medical advances, and the elimination of rule-based, routine work. A 2016 report by the White House Office of Science and Technology Policy says "The current wave of progress and enthusiasm for AI began around 2010, driven by three factors that built upon each other: the availability of big data from sources including e-commerce, businesses, social media, science, and government; which provided raw material for dramatically improved machine learning approaches and algorithms; which in turn relied on the capabilities of more powerful computers."

Given the potential benefits and risks, what do agency risk managers need to know to better understand the AI landscape? First, they should understand what is AI; then . they should identify potential uses and implications of AI for agencies and their missions; and finally, they should be aware of the categories of risk related to use of AI with respect to their overall enterprise risk portfolios.

What Is Artificial Intelligence? The term "artificial intelligence" is not a single technology. It is a broad field of different types of technologies, used for different purposes. The Cambridge Centre for the Study of Existential Risk observes "Most current AI systems are 'narrow' applications – specifically designed to tackle a well-specified problem in one domain, such as a particular game. Such approaches cannot adapt to new or broader challenges without significant redesign. While it may be far superior to human performance in one domain, it is not superior in other domains. However, a long-held goal in the field has been the development of artificial intelligence that can learn and adapt to a very broad range of challenges."

Today, AI is used to develop in fields such as vision (e.g., facial recognition), robotics (e.g., retrieving orders in warehouses), natural language (e.g., call center responses),

machine learning (e.g., fraud detection), automated planning and programming systems (e.g., managing construction projects), and rule-based expert systems (e.g., processing insurance claims).

The fears stirred by popular literature on AI focuses on the creation of "super intelligence" that exceeds human performance in nearly all domains – science, arts, military, economy, security, etc. While this may be a future concern, and there are scientists and ethicists pondering these issues, we are not there yet. This article focuses on current and near-term implications for agency risk managers.

Given the varied types and uses of AI, defining it is not straightforward, but a key distinction is that machine learning is based on increasingly complex mathematical algorithms that are used to make predictions.

Limitations of AI. Given that AI is rooted in algorithms and data, there are a number of limitations to its use, at least in the near term. Key in these limitations are the lack of transparency in how AI makes its predictions, and that AI is currently limited to specific uses.

An article by Cary Coglianese and David Leher says that "AI is different than traditional statistical techniques which seek to model underlying data-generating processes, and this limits the transparency of how a decision is made. Machine learning is non-parametric – that is, the data dictates how information contained in input variables is put together to forecast value of output variable – rather than a human-defined statistical model that uses data to validate or reject a hypothesis."

As a result, the causal inferences of statistical modeling typically cannot be applied to the results of machine learning. Thus, options are seen as being developed in a "black box" without a justification for how the answer was derived. Another consideration with respect to use of AI in decision-making is administrative law, which requires justifications for decisions, especially those that affect individual freedoms. Newer technologies are on the verge of overcoming this weakness in some uses of AI, but a risk manager needs to explicitly ask.

AI is currently limited to specific, defined uses; and if applied to uses other than what it is designed, will produce errors. James Hendler and Alice Mulivhill, in their 2016 book *Social Machines*, note that computers can process large amounts of text with their large memories and use specialized algorithms to identify items hard for humans to identify in images (e.g., x-rays). However, a computer cannot identify a context. For example,

doctors can take into account context when they analyze an x-ray, and based on their experience, they can include insights beyond medicine when prescribing their treatments.

Some tasks that are easy for humans, are hard for computers. For example, object recognition in a particular context. Humans have the ability to reason across contexts (e.g., child, duck, airplane) but so far computers do not. In contrast, tasks that are hard for humans, are easy for computers, such as rules-based reasoning or sorting through millions of options when playing chess. Users must be very specific in defining what problems to address with AI and how AI algorithms are to be trained to address specific issues, or the AI will result in errors.

As James Wilson and Paul Daugherty write in a recent *Harvard Business Review* article, "While AI will radically alter how work gets done and who does it, the technology's larger impact will be in complementing and augmenting human capabilities, not replacing them." An AI expert at IBM, Claude Yusti, emphasizes that "AI is not a decision-making engine, but an assistant to humans." He cautions that AI is not sufficiently mature to be applied for independent decision-making, and that AI may not be the right tool for a specific use.

Potential Uses of AI in Government. Even with the limitations noted above, AI has concrete, specific uses. The Forbes Technology Council describes eleven ways that government is, or could be using AI. Most of the potential uses they identify support rule-based work processes such as the following:

- Managing case loads
- Recruiting staff
- Ensuring safety
- Ensuring cybersecurity
- Computing taxes
- Operating HR systems
- More efficient auditing

In addition, some types of uses take advantage of natural language or machine learning algorithms, such as:

- Comment response filtering
- Irregular financial activities
- Human behavior imitation (e.g., therapy support)

Other uses are linked to specific mission tasks (e.g., gas pipeline inspections, flight paths) that rely on software that automates planning and programming processes.

A recent report on the use of AI in government by the Partnership for Public Service and the IBM Center for the Business of Government, describe several case studies of how AI is used in several agencies. For example, the Bureau of Labor Statistics uses AI to relieve employees of the tedious and repetitive task of reading survey responses to identify important details to code in a database. By allowing a computer and AI to assign codes to pieces of survey information, it saves employees hundreds of hours of work, and they can focus on higher-level analytic tasks.

Near-Term Implications of AI in Government. *Federal Computer Week* reports that, as part of its drive to reduce "low value work," . . . "the White House estimated 5 percent of federal government occupations could be "automated entirely," and 60 percent could have at least 30 percent of their activities automated. The administration estimates that 45 percent of "total work activities" could be automated governmentwide."

But Wilson and Daugherty write that automating work does not necessarily mean that work will be eliminated. They conclude that "[m]ost activities at the human-machine interface require people to *do new and different things* (such as train a chatbot) and to *do things differently* (use that chatbot to provide better customer service)." This implies new investments in training and retraining employees. This is happening in the corporate world much more quickly than in the government world.

Some Challenges Where Risk Should be Assessed. Risk managers should be attuned to both the technical and the non-technical challenges of agencies deploying AI in their mission space.

Examples of some potential technical risks of AI include the following:

- Data quality and potential for unconscious bias
- Role of algorithms – black box vs. having the technical talent to deconstruct math to provide transparency into how an algorithm arrived at a decision – which is made more difficult when using proprietary code
- Overcoming the challenges of legacy systems, system and data interoperability, and data sharing

Another key technical risk – or benefit – is AI's role in cybersecurity. It can be a tool to help, or in the wrong hands, it could be a powerful tool to penetrate systems.

Some potential non-technical risks of AI are as follows:

- Recruiting and retaining employees with skillsets needed to develop, manage, and oversee AI operations and usage
- Ethical and legal considerations (e.g., privacy, security, due process, delegating autonomous decisions on life-or-death situations)
- Impact on the greater workforce and/or workplace
- Impact on processes - need to develop new business and governance models
- Over-reliance in decision-making

Another important non-technical risk to consider is that, because most program managers and contract officers do not understand AI, they don't know how to acquire it. It is classified as a "skilled acquisition requirement." As one observer puts it, "It's like someone who has never driven before, being asked to buy and drive a Ferrari – you don't know what it can or cannot do." It takes someone with a certain level of technical knowledge to understand if AI is the appropriate solution to apply to a specific business use.

Kevin Desouza, in a recent report for the IBM Center, identifies several additional types of risks and mitigation strategies, such as ensuring interconnected systems are secure; avoiding a "wait-and-see" approach; and introducing a governance approach earlier rather than later to develop policies and standards before significant investments are made.

Monitoring Longer-Term Potential and Risks of AI. The longer-term potential and risks of AI are under examination by a number of groups inside and outside government. Their work will provide insights to risk managers down the road. One example of these groups is the non-profit AI research company OpenAI, created in 2015 by a consortium of technology companies and individuals who committed $1 billion to "discovering and enacting the path to safe artificial general intelligence." It has a staff of 60 and sponsors research and conferences to define and ameliorate potential harms, as well as to test different AI approaches. Similar strategic study efforts are being undertaken by organizations such as DeepMind and the Centre for Human-Compatible AI.

At the U.S. federal level, a recent Government Accountability Office report on the emerging opportunities and challenges of AI highlights a series of policy issues and research priorities that need to be addressed in coming years. These include regulatory, risk, and ethical considerations. Along with these non-technical issues, the technical

issues noted earlier of moving beyond existing legacy IT systems, the interoperability of IT systems, and the sharing of data sets are also areas requiring the attention of both leaders and risk managers.

While the risks are still being defined, the benefits are already coming to fruition. For example, the World Economic Forum sees the value of hybrid networks of humans and machines that sense, think, and act collectively versus humans or AI systems alone. By engaging both AI and 30,000 human volunteers, citizen science platform stardust@home discovered five interstellar dust particles hidden among a million digital images, and a network of online gamers are interacting with AI to help accelerate a cure for Alzheimer's disease.

John Kamensky is a senior fellow with the IBM Center for the Business of Government in Washington, DC. He is also a fellow of the National Academy of Public Administration. He is a former government executive, having served in the Government Accountability Office and the Office of Management and Budget.

AFERM's Small Agency Community of Practice

Supporting Small Agencies' ERM Pursuits

The ERM Small Agency Community of Practice (SACoP) is a Federal-only forum where practitioners come together to share their experiences and learn from each other as we navigate the unique challenges of enterprise risk management in a small agency setting. Starting in FY19, meetings will be held monthly with guest speakers, Industry Days, and agency presentations on relevant topics. A schedule of next year's meetings is coming soon and will be posted to the AFERM calendar.

For more information or to join SACoP, please reach out to **Valerie Lubrano** at aferm.sacop@gmail.com

AFERM Membership

Membership Provides Access to Valuable Resources

With over 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 AFERM.membership@gmail.com.

Request for Your Success Stories or Thought Leadership

Communicating the Value of ERM

We'd like to hear from you on your experiences in leading or supporting risk management efforts. Please send a short description to the AFERM Communications team. We hope to accumulate a series of vignettes that will support continued interest in the benefits of ERM throughout the Federal government.

In addition, we are willing to work with new or established authors to publish thought leadership articles in future editions of this Newsletter. Guidelines will be provided to interested parties.

Please send your success stories or request for information on publishing a thought leadership piece to the AFERM Communications Committee at AFERM.Communications@gmail.com. The Committee is responsible for the AFERM Newsletter and is led by **Shelly Turner** with **Andrew Glover and Nadya Korobko** of Guidehouse.

2019 AFERM Officers, Committees, and Communities

Officers
President, Tom Brandt
Past President, Peggy Sherry
President-Elect, Ken Fletcher
Treasurer, Fola Ojumu
Secretary, Mike Wetklow
VP at Large, Harold Barnshaw
VP at Large, Ed Hau
VP at Large, Sean Vineyard

Corporate Advisory Group (CAG)
Cynthia Vitters, Deloitte
Brian Barker, Ernst & Young
Nicole Puri , Grant Thornton
David Fisher, GuideHouse
David Zavada, Kearney & Company
Tim Comello, KPMG
Sean Vineyard, 11th Hour Service
Maurice Cesa, ACL
Jeannine Rogers, AOC Solutions
Jennifer Gordon, Castro & Co.
Bert Nuehring, Crowe LLP
Dr. Natalie Houghtby-Haddon, George Washington University
Tim Mobley, IRIS Intelligence
Shawn O'Rourke, Pro-Concepts
George Fallon, RMA Associates, LLC
Carrie Everett-Vaughan, RSA
Sim Segal, SimErgy Consulting
Rob Crawson, Sword Risk Manager
Kim Milne, WAEPA

CAG Liaison
Werner Lippuner

Audit
Sheri Francis, Chair
Ed Hau

Bylaws, Policies and Procedures
Mike Wetklow, Chair

Bylaws, Policies and Procedures
Mike Wetklow, Chair

Communications
Shelly Turner, Chair
Andrew Glover
Nadya Korobko

Cyber ERM Community of Interest
Nahla Ivy, Chair

Data Analytics Community of Interest
Curtis McNeil, Chair

Finance/Budget
Fola Ojumu, Chair

Knowledge Capital
Brian Murphy, Chair
Tim Weber

Membership
Yehuda Schmidt, Chair
Domenyck Schweyer

Outreach and Advancement
Sean Vineyard, Chair

Planning
Christina Girardi and Marc Pratta

RIMS Liaison
Cynthia Vitters

Summit Committee 2019
Nicole Puri and Meredith Stein

Small Agency Community of Practice
Valerie Lubrano, Chair

Volunteer
Laurence Mazella

Corporate Sponsors

Thank You for Your Support!

Platinum Sponsors

Deloitte.

EY Building a better working world

Grant Thornton

Guidehouse. formerly PwC Public Sector, LLP

KEARNEY & COMPANY

KPMG

Silver Sponsors

11TH HOUR SERVICE

acl

ARM Active Risk Manager

AOC SOLUTIONS

Castro & Company Auditors ✓ Advisors

Crowe

GW

IRIS INTELLIGENCE

MORGANFRANKLIN CONSULTING

Educational and Professional Certification Sponsors