AFERM
Association for Federal
Enterprise Risk Management

AFERM Newsletter

Issue 35
December 2020

Thought Leadership for the Federal Enterprise Risk Management Community

Contents

Highlights

This 35th issue of the quarterly AFERM Newsletter includes thought leadership articles from ERM practitioners with ASR Analytics, Bureau of the Fiscal Service, National Institutes of Health, Office of the Comptroller of the Currency, and U.S. Customs and Border Protection.

The President’s Corner

AFERM President Nicole Puri

AFERM in 2021

By Nicole D. Puri, AFERM President

As our society finds itself in month 11 of the pandemic, many of us continue to hunker down and try to stay motivated despite the restrictions. One thing I have realized as I start my term as President is how difficult it is to mark progress when the days feel indistinguishable from each other. However, we now have some hopeful signs of the return of normal activities, and meanwhile, the AFERM Board and committees have been hard at work to make sure this year is a productive one.

For some time, AFERM has been working on a new Strategic Plan and considering operating model changes that will allow us to make better use of our volunteers. These are long-term structural changes which I believe will further strengthen AFERM’s ability to provide you with the activities and content you value. In addition to potentially changing our operating model, a few major initiatives are underway, including publication of a federal ERM standard and creating new opportunities for members which will help diversify AFERM’s revenue base. We also have several ideas in the works to add some significant benefits for our sponsor community.

Many of us are also preparing for a transition in administration and what that will mean for our ERM work. Though too early to say how the new administration will look upon ERM, we at AFERM remain hopeful and will be looking for opportunities to demonstrate the value and importance of ERM in the federal government. I would love to hear from our members about opportunities that they have seized to share ERM as we move further into the transition, so that I can share those with a wider audience.

Finally, I encourage you to check out an interview recently conducted by Federal News Network with David Fisher and me on the results of the AFERM-Guidehouse ERM 2020 Survey, which was released during the AFERM Summit in September 2020. In the interview we explored themes related to ERM risk culture, the connection between internal controls and ERM, and where agencies have made advancements.

AFERM continues to work hard for you, our members and sponsors, and we look forward to a great year together! As always, if you have something you would like to discuss with me, please don’t hesitate to reach out to me.

Happy New Year!

Nicole D. Puri

____

Nicole Puri, AFERM President, may be contacted at President@AFERM.org.

EFFECTIVE TOOLS TO INFORM LEADERS
AOCSolutions
Service Disabled - Veteran Owned
www.aocfederalsolutions.com

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:

- **Nicole D. Puri**, AFERM President, and CRO at the Bureau of the Fiscal Service
- **David L. Fuller, II**, Senior Management Analyst, National Institutes of Health
- **Marty G. Meyer,** Chief Engineer and CRO, **Dr. Gunter Brunhart,** Technical Director and Branch Chief for Engineering Management, **Dr. Steven Moyer,** Deputy Chief Engineer and Deputy CRO, and **Dr. Richard Dubs**, Workforce and Knowledge Management Subject Matter Expert, U.S. Customs and Border Protection, and **Thomas Erickson, Robert Skalamera, and Rob Kepner,** contractors to CBP
- **Ed Hau**, Director, ASR Analytics, and **Harold Barnshaw**, AFERM Vice President at Large and Director of Accounting, Office of the Comptroller of the Currency

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@guidehouseFederal.com and nkorobko@guidehouseFederal.com, respectively.

Thought Leadership

Cloud services: An ERM perspective

By David L. Fuller, II, J.D.

In 2019, the Government Accountability Office (GAO) reported that the Federal Government spent nearly $90 billion on information technology (IT) procurements.[1] Of those procurements, nearly $6 billion were spent on cloud services.[2] Cloud computing presents the Federal Government with an enterprise opportunity to transform inefficient, outdated, or inflexible information systems into more flexible, nimble, and efficient IT services.[3] The need for a nimble IT infrastructure has become more relevant by the COVID-19 pandemic and social distancing needed to combat the spread of the virus. As we move forward into a new decade, government agencies will need to continue to update and improve their information systems by investing in cloud services. However, the adoption of cloud capabilities exposes agencies to potential risks as well. This article discusses a few of these risks and mitigating actions that an agency may consider as it relates to cloud services.

David L. Fuller, II

1. Defining Cloud Services

Risk Statement: If an agency does not clearly define “cloud services,” it runs the risk of acquiring services that do not further its mission and objectives and that are not compliant with Federal requirements.

Mitigating Action: Define “cloud services” for the agency.

Everyone has a different meaning for cloud services. For some, the cloud is just the new way to access email or watch movies. For others, the cloud is a new way to save on storage space or increase computing power. This disparate view of cloud services presents challenges in effectively implementing agency-wide cloud services. Without a clear vision of cloud services for the agency, work units run the risk of acquiring services based on their own unique needs instead of aligning with the agency’s overall cloud services strategy.

[1] Government Accountability Office Report: *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked* GAO-19-58, May 2019

[2] Bloomberg Government Report: *The State of Federal Cloud,* December 2019

[3] Government Accountability Office Report on *Cloud Computing, Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, GAO-16-325, April 2016.

The National Institutes of Standards and Technology (NIST) defines cloud computing as "…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[4]

The NIST definition is a broad definition designed to capture all aspects of cloud computing. In 2019, the Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, published the Federal Cloud Computing Strategy. This strategy emphasizes the need for agencies to consider their mission and objectives needs, technical requirements, and existing policy limitations.[5] When an agency is adopting cloud services, it is important to have a uniform definition of cloud based on the agency's mission and objectives. Technical requirements are unique to each agency and should be considered when defining the use of cloud services. In addition, by developing a clear definition, you are also better able to understand how current policies and procedures support or limit the use of cloud services to ensure compliance throughout the agency. When an agency establishes a common definition for cloud services and effectively communicates this agency-wide, it will best position itself to acquire cloud services that will further its mission and objectives and ensure Federal compliance.

2. *Cloud Services Inventory*

Risk Statement: If an agency does not maintain a complete inventory of cloud services, then it is unable to provide an accurate account of cloud services for reporting, tracking, and auditing purposes; hinders its ability to make informed strategic decisions; and neglects its duty to protect sensitive data.

Mitigation Action: Conduct an inventory of existing cloud services.

According to NIST, Federal agencies need to develop and document an inventory of information system components that: (1) Accurately reflects the current information system; (2) includes all components within the authorization boundary of the information system; and (3) includes the granularity deemed necessary for tracking and reporting.[6] In addition, the Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government*, or "Green Book," states, "[d]ocumentation provides a means to retain organizational knowledge and a means to communicate that knowledge as needed to external parties such as external auditors."[7] Maintaining a complete centralized inventory of cloud services and vendors increases the ability of an agency to provide an accurate account for reporting, tracking, and auditability. Ensuring the

[4] Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011.

[5] Federal Cloud Computing Strategy, June 2019.

[6] NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

[7] GAO Standards for Internal Control in the Federal Government, Green Book, September 2014.

accuracy of this information allows the agency to effectively meet Federal reporting and auditing requirements and reduces its risk of non-compliance.

Another benefit of conducting and maintaining an inventory of cloud services is to increase an agency's ability to make informed strategic resource decisions. For example, if two or more offices are utilizing similar cloud services, an agency can use this information to take an enterprise approach to procure a more cost-effective cloud solution. Making informed strategic resource decisions, minimizes redundancy, reduces costs, and leverages the agency's economy of scale allowing it to better achieve its mission and objectives related to cloud services.

Finally, without an inventory of cloud services, an agency's ability to protect sensitive data is impacted due to a lack of oversight of which systems are in the cloud and whether those systems contain sensitive data. According to the Privacy Act of 1974, the Federal Government has the responsibility to protect the privacy of sensitive information. "Each agency that maintains a system of records shall…establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[8] By not maintaining an inventory, the agency does not have a clear understanding of the information that is at risk for exposure and is unable to be good stewards of the information they are at duty to protect.

3. Intra-agency Cross Collaboration

Risk Statement: If an agency does not emphasize the need for cross collaboration, then it is unable to address the internal learning curve associated with purchasing and managing cloud services.

Mitigating Action: Promote a culture of intra-agency cross collaboration.

Cloud services is a relatively new product and there are few standardized practices across vendors. Each vendor is trying to provide something better than the next. The different services provided by vendors are vast and constantly changing. The Federal Government is still learning how to apply this new technology to existing processes to achieve mission goals and objectives, meet technical requirements, and comply with regulations. As such, there is a learning curve within the Federal Government related to integrating cloud services and inter-agency collaboration is an important component that can be used to address this.

For program managers, the learning curve is about how best to use cloud services to accomplish program objectives. Program managers must understand the difference in cloud platforms and the function of each platform compared to what the program area is

[8] The Privacy Act of 1974, 5 U.S.C. § 552a, December 1974.

trying to accomplish. For acquisition officials, they need to understand the cloud marketing structure, appropriate contract vehicle, and funding types necessary to acquire appropriate cloud services from an enterprise perspective. Additionally, IT officials must understand the security, operation, and performance requirements of each cloud platform needed in order to provide support to program areas and acquisition offices. Finally, agency management must understand all these areas to provide oversight and guidance in the purchasing and management of cloud services. Because of the interdependencies of each of these stakeholders, cross collaboration is key in addressing the learning curve of dealing with this new industry. Promoting a culture of intra-agency cross collaboration early on lessens the learning curve by ensuring the appropriate knowledge and expertise about the function, management, and requirements of cloud services are shared across the agency in order to establish an enterprise approach.

4. Supplemental Contract Language

Risk Statement: If an agency does not address vendor lock-in, data ownership, pricing structure, Federal Risk and Authorization Management Program (FedRAMP) authorization, and service level agreements within a cloud services contract, it increases its risk of not being to ensure cost effectiveness, performance, or compliance with Federal contracting regulations.

Mitigating Action: Use supplemental contract language to address vulnerabilities.

As the Federal Government is integrating cloud services across agencies, several considerations must be addressed with regard to acquiring these services. Acquisitions plays an integral role in the support of a strong cloud services strategy. To protect the Government's interest in acquiring cloud services, acquisitions programs will have to ensure cloud services contracts are in compliance with Federal security and contracting regulations, are cost effective, and meet the performance requirements the agency needs. As such, an agency should consider using supplemental contractual language to address vulnerabilities specific to cloud services such as vendor lock-in, pricing structure, security requirements, data ownership, and service level agreements.

<u>Vendor Lock-In.</u> Addressing vendor lock-in is about ensuring the agency can retrieve their data from the vendor in a useable format at the end of the contract. An agency increases the risk of being committed to one vendor regardless of cost or performance when data cannot be transitioned back to the agency. This typically happens when a vendor develops its own system or technology to serve as a select fit for what the government agency needed at that specific time. For example, a government agency uses Vendor A's cloud services and products but cannot transfer to Vendor B's services or products without a significant investment of time and money, or loss of data. To mitigate the risk of vendor lock-in, an agency should include supplemental language to ensure the vendor assists in transition efforts at the end of the contract such as the extraction of data and the transfer of data to the agency in a useable format.

Data Ownership. Supplemental language regarding data ownership is important as it allows the agency to determine that the agency maintains the rights to data collected in order to safeguard the data and ensure proper use of that data. This is in accordance with both the Privacy Act of 1974 and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002[9] and its reauthorization in 2018 which requires all Federal agencies to, in part, "…*protect the trust of information providers by ensuring the confidentiality and exclusive statistical use of their responses."*[10]

Similar to vendor lock-in, an agency should be explicit in the contract about the ownership of the data in the cloud. The contract should include language about the agency's right to retain unrestricted access to or ownership of any data collected, stored, maintained, used, or operated on behalf of the agency on the vendor's cloud services infrastructure to ensure compliance with Federal laws and regulations.

Pricing Structure. The greatest risk an agency should mitigate regarding pricing structure is a violation of the Antideficiency Act (ADA) which states that Federal Government may not "…make or authorize an expenditure or obligation exceeding an amount available in an appropriation or fund for the expenditure or obligation."[11] There are multiple ways an agency can set up the pricing structure for cloud services (e.g. firm-fixed price, pay-as-you-go, time and materials, etc.) but each run the risk of violating ADA requirements if not properly monitored. By not monitoring cloud usage, the agency runs the risk of exhausting funds prior to the payment period which will force them to incur an over-obligation in violation of the ADA.

Supplemental language regarding monitoring cloud usage is critical in helping to mitigate this risk. For instance, an agency could require a vendor to provide updates or reports on a continual basis regarding cloud usage or could request that the vendor report back before moving forward when a specific threshold has been met. Supplemental language within the contract stipulating these requirements around monitoring cloud usage will help ensure efficient management for both cloud services usage and expenditures and reduce the likelihood of ADA violations.

FedRAMP Authorization. Supplemental language requiring vendors be FedRAMP authorized is critical to include within cloud contracts in order to protect an agency's IT infrastructure and to ensure compliance with Federal cloud IT regulations. In December 2011, FedRAMP was established to provide a government-wide, standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[12] Prior to FedRAMP, vendors were faced with complying with different requirements for different agencies.[13] With the establishment of FedRAMP, OMB

[9] Confidential Information Protection and Statistical Efficiency Act of 2002
[10] Reauthorization of Confidential Information Protection and Statistical Efficiency Act of 2018
[11] Antideficiency Act
[12] FedRAMP – About Us
[13] FedRAMP – Cloud Service Providers

mandated FedRAMP compliance for all new cloud services used by Federal agencies in order to "…reduce duplicative efforts, inconsistencies, and cost inefficiencies associated with the security authorization process."[14] Therefore, in order to ensure compliance with the FedRAMP mandate that any cloud services that hold Federal data be FedRAMP authorized, supplemental language detailing this requirement should be standard practice.

Service Level Agreements. Service level agreements (SLA) document the performance level for compliance with the contractual agreement and play a critical role in ensuring Federal agencies receive the services they are paying for in a timely manner. Within a cloud services contract, an SLA can be used to define performance expectations related to monitoring and reporting usage; data storage, use, and management; and contract closeout provisions. If an agency fails to include language related to vendor performance and expectations in the establishment of an SLA, then the agency may not be able to ensure that the vendor meets adequate service levels which increases the risk that agencies could misspend or ineffectively use funds.[15] In addition, agencies may not have recourse to impose penalties or address inadequate performance if the terms of the SLA do not effectively detail performance requirements. Therefore, it is important that the agency ensures the SLA clearly addresses cloud services performance requirements in line with the agency's overall cloud services strategy.

In closing, the use of cloud services presents several benefits to the Federal Government including cost savings, improved security, and delivering faster services.[16] However, to fully reap these benefits, there is a need for proactive thought in order to develop a strategic cloud services vision. Being strategic will not only ensure an enterprise approach to cloud capabilities but will also help to identify associated risks. Addressing these risks will allow agencies to fully achieve the benefits of cloud computing and effectively develop a more nimble, efficient, and effective IT infrastructure in order to better achieve agency mission and objectives.

David Fuller, II may be reached at fullerd@mail.nih.gov.

Mr. Fuller works as a Senior Management Analyst at the National Institutes of Health (NIH), Office of Management Assessment in the Risk Management Audit Liaison Division. In this capacity, he is responsible for overseeing NIH-wide internal control assessments and providing support to the NIH's overall risk management strategic planning, communication, and training activities.

The views expressed are his own and do not represent the views of the National Institutes of Health or the United States Government.

[14] Memorandum for Chief Security Officers, *Security Authorization of Information Systems in Cloud Computing Environments*. December 8, 2011.
[15] Council of the Inspectors General on Integrity and Efficiency, *The Council of the Inspectors General on Integrity and Efficiency Cloud Computing Initiative*, September 2014.
[16] OMB, Federal Cloud Computing Strategy

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
The Foresight Sandbox February: Strategic Foresight Training for an Era of Accelerating Change	Prescient	February 16-17, 2021	Virtual
Virtual AFERM & AGA 2021 ERM Workshop	AFERM and AGA	April 14, 2021	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.

AFERM's ERM Podcasts

AFERM's podcasts continue the ERM dialogue

Be sure to check out the 40 Risk Chat podcasts on our website featuring ERM subject matter relevant to the Federal sector. If you are interested in participating on a podcast, please contact Paul Marshall, MILCorp, and Tal Seaman, Navigator Solutions.

The Risk Chat podcasts are accessible on AFERM's website at https://www.aferm.org/aferm-risk-chats/. The most recent five (5) podcasts are listed below with active links.

- Episode 40: RIMS-CRMP-FED Certification
- Episode 39: Higher Education ERM
- Episode 38: ERM Around the World
- Episode 37: Operationalizing USAID's Risk Appetite Statement
- Episode 36: AFERM President Ken Fletcher

Paul Marshall may be contacted at pmarshall@milcorp.com, and **Tal Seaman** may be contacted 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. Those listed below include active links to each article.

- How to Make the Most Out of 2021's Virtual Conferences for Rising Risk Professionals and Employers
- Covid-19 and the Next Generation of Risk Management
- Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks, Dec 15, 2020
- A Broader View of Construction Risk Management
- Year in Risk 2020
- Rethinking Risk in a Post-Pandemic World
- Risks To Watch In 2021
- Cyber Risk Management in the Pandemic Era
- Managing Risk in the Public Sector
- CPRA and the Evolution of Data Compliance Risks
- Compliance Operations During Covid-19
- Fewer Companies Taking Cyberrisk Mitigation Steps
- Evolving the ERM in Government: Reflections of a Risk Management Professional

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.

Guidehouse

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

Follow Us Online **@Guidehouse**

Thought Leadership

Agile risk tolerance: A novel approach for government acquisition and procurement

By Marty G. Meyer, Dr. Gunter Brunhart, Dr. Steven Moyer, and Dr. Richard Dubs of U.S. Customs and Border Protection (CBP) and Thomas Erickson, Robert Skalamera, and Rob Kepner, contractors to CBP

Introduction

In 2015, the Commissioner of CBP sponsored the Defense Acquisition University (DAU) in reviewing CBP's acquisition and procurement performance. As a result, DAU offered 66 recommendations to CBP leadership, including two related to risk that were accepted and assigned for implementation:

- "Set the tone for more risk tolerance
- Reward innovation and risk, not punish failure"[17]

CBP recognized the two recommendations on risk have the promise of significantly improving schedule and cost performance of the government acquisition process. This article proposes an Agile Risk Tolerance (ART) process based on the two DAU recommendations and describes CBP's approach for implementing it.

What is Risk Tolerance?

Tolerance in common language is well understood. One dictionary definition calls tolerance "the act of enduring, or the capacity for endurance[18]." Tolerance is not a new concept in risk management. International Organization for Standardization (ISO) Guide 73 defines risk tolerance as an "organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives[19]." The Committee of Sponsoring Organizations of the Threadway Commission (COSO) ERM Framework defines risk tolerance as "the acceptable variation relative to the achievement of an objective[20]."

These three definitions have in common the concept of enduring an event or condition. Thus, if we are risk tolerant, we are willing to endure the likelihood of an uncertain event or condition and its possible impacts. Conversely, to say we are not risk intolerant is to say we are unwilling to endure a future event or condition or its potential impacts.

[17] Defense Acquisition University. Outbrief - Review of Customs and Border Protection (CBP) Acquisition Program (2015, p30)

[18] *Standard College Dictionary.* (New York: Funk and Wagnalls Company, 1963.

[19] *ISO Guide 73 Risk management – Vocabulary* (International Standards Organization. 2009)

[20] *Enterprise Risk Management – Integrated Framework. Executive Summary – Framework.* (The Committee of the Sponsoring Organizations of the Treadway Commission (COSO). 2004)

In 2016 CBP addressed the specific DAU recommendations through chartering a multi-year Acquisition Management Performance Improvement (AMPI) initiative, organizing 13 teams under six executives charged with addressing 38 of the 66 recommendations and deferring two and closing the other 26. One of the teams led by the CBP Chief Engineer was tasked to address the two risk management recommendations cited above.

Game Plan for Increasing Risk Tolerance

The Risk Tolerance Team (the "Team"), quickly realized their success in implementing the two risk recommendations faced two significant hurdles:

1. Progress Measurement: Tolerance is largely a qualitative concept. When you say one individual – or government agency – is more risk tolerant than another, it is a largely qualitative comparison. It is difficult to measure change in qualitative terms, at least in terms that are universally understood and accepted and not subject to bias, interpretation, or hidden agendas.
2. Culture Change: Risk intolerance can be deeply ingrained in government agencies.[21,22,23] It would not be enough to encourage the rank-and-file to take more risks if the support is not there from the top to the bottom of the organization; and acceptance and support of risk tolerance practices by leadership is critical as well.

To address these hurdles, the team developed a strategy with eight goals, presented in the table below.

Table 1: Team Strategy

Goal	Description
Best Practice Refresh	To collect best practices that show effective handling of risk to include researching potential enterprise tools that could be used to track metrics and establish success against best practice benchmarks.
Performance Metrics	To define long term performance criteria to monitor the health of CBP risk and innovation in acquisition, and to identify and mitigate adverse practices that would decrease risk tolerance.

[21] There are a few exceptions, the Defense Advanced Research Projects Agency and the National Aeronautics and Space Agency are perhaps the most well-known, but they do not control a large percentage of the federal budget. NASA's FY2020 budget of $22.5B is only 0.4% of the Federal FY2020 $4.8 *trillion* budget (NASA 2020). DARPA's budget is even smaller, at $3.556 billion (DARPA 2020).

[22] NASA. 2020. "NASA Budget, Current Funding, History, and Economic Impact". Last modified February 27th. https://www.thebalance.com/nasa-budget-current-funding-and-history-3306321.

[23] DARPA. 2020. "Budget". Last modified March 2019. https://www.darpa.mil/about-us/budget.

Goal	Description
Process	To establish a methodology for introducing innovation and risk tolerance in existing risk management practices.
Workshops for Rollout	To provide training and learning opportunities on methods for identifying and mitigating risk and apply this to the acquisition function (Portfolio Acquisition Executives and Program Managers).
Reward Program	To develop a framework of awards and rewards for acknowledging acquisition and procurement management (and teams) that smartly take risk and innovate.
Expand Risk Staff Outreach	To create a robust mentoring/pairing system where staff who are adept at managing risk can help those who are less so, and to identify other Agency practitioners that can mentor/support the acquisition community.
Communication Plan	To build and launch a communication program to market training, documentation updates, and the reward program.
Policy	To establish directives to set expectations and implement required changes.

Measuring Progress

“If you can’t measure it, you can’t improve it,” Peter Drucker.

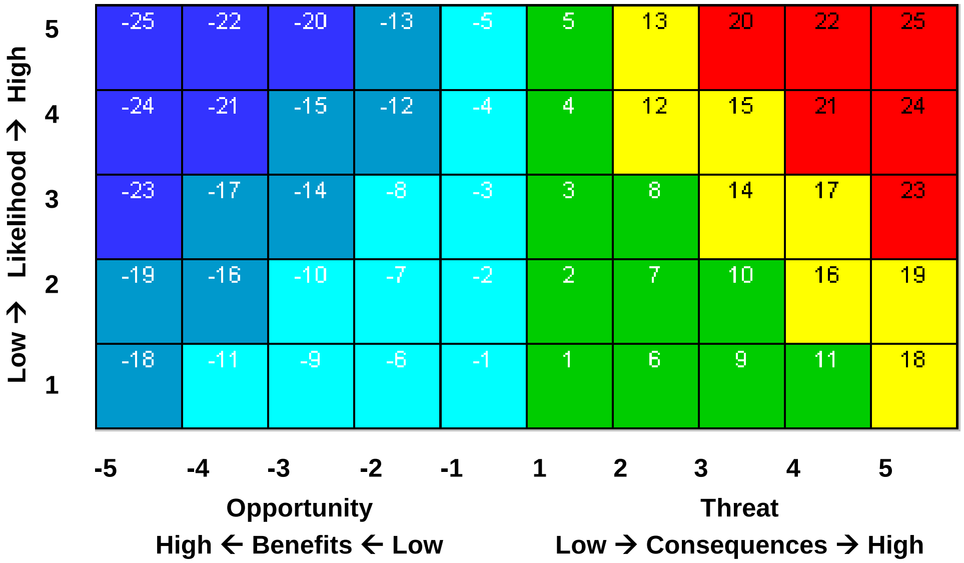
In commencing work on the first two goals – capturing Best Practices and establishing Performance Metrics, we quickly discovered that there were not many best practices published which we could consider and that CBP needed a means of quantitatively measuring change in risk tolerance. However, CBP had in place traditional risk management techniques for measuring and recording risk impact that could be leveraged for relating risk assessment to risk tolerance.

The CBP Office of Acquisition (OA) encourages all risk practitioners to prepare two impact assessments in determining whether to address an uncertainty and how much effort to put into that response. The first assessment measures how much impact the uncertainty could cause to organizational goals and objectives if nothing is done. In common risk management terminology this is called the ***inherent risk*** assessment. The second assessment measures the potential impact of the uncertainty after treatment is complete, and it is called the ***target risk*** assessment. By the definition of uncertainty, there is always a chance the uncertainty may occur despite best efforts. The remaining potential impact after treatment is known as the ***residual risk***.

Inherent risk is used to decide whether to treat the uncertainty, that is, whether to focus effort on changing the uncertainty’s likelihood and/or impact. Frequently, organizations establish thresholds of inherent risk that must be crossed before it is worthwhile to organize and execute treatment. Such thresholds define the organization’s ***risk appetite***.

As the treatment plan unfolds, impact assessments are conducted to measure progress. These are called ***current risk*** assessments, and they are used to decide when the treatment may stop. Stated another way, when the current risk assessment results match the target risk assessment results, the organization is willing to accept the residual risk, and if necessary, execute any fallback (contingent) actions if the uncertainty in fact unfolds.

CBP’s OA assesses risk impact qualitatively using a five-point scale for likelihood, opportunity, and threat. A unique number from 1 to 25 is assigned to each cell of the resulting five-by-five Probability/Impact Diagram (PID). (See Figure 1 below.)



	-5	-4	-3	-2	-1	1	2	3	4	5
5	-25	-22	-20	-13	-5	5	13	20	22	25
4	-24	-21	-15	-12	-4	4	12	15	21	24
3	-23	-17	-14	-8	-3	3	8	14	17	23
2	-19	-16	-10	-7	-2	2	7	10	16	19
1	-18	-11	-9	-6	-1	1	6	9	11	18

Figure 1 Probability/Impact Diagram

In this standard PID, threat impacts are designated on the right and opportunity impacts are designated on the left. For threats, consequences increase moving up and to the right and decrease moving down and to the left. Inherent risk assessments are closer to the upper right corner than target assessments. For opportunities, benefits increase moving up and to the left. Inherent risk assessments are closer to the lower right corner than target risk assessments[24].

We discovered that the difference between the inherent risk assessment and target risk assessment could be used to indicate the organization’s tolerance for a given uncertainty and its potential impacts, and that an aggregation of these differences for all

[24] This numbering scheme is driven even today by the common but incomplete belief that all risks are threats and thereby may be more conveniently conveyed with positive numbers, leaving opportunities as negative numbers to balance overall risk (threat and opportunity) exposure.

the uncertainties across the organization could be used as an indicator of overall risk tolerance. The *greater* the difference between inherent and target threat assessments, the *less* risk tolerant the organization was. The *greater* the difference between inherent and target opportunity assessments the *more* risk tolerant the organization was.

Furthermore, the differences between inherent and target risk assessments reflect where the organization wants to allocate its risk management resources. An organization that allocates the greater part of its risk management resources to “burning threats down to zero” is the very definition of a risk intolerant organization as it indicates it cannot tolerate much residual risk.

A simple count of all active and closed threats (risks), issues, and opportunities to date in CBP’s de facto common risk management database reinforces the DAU findings. (See Figure 2 below.)

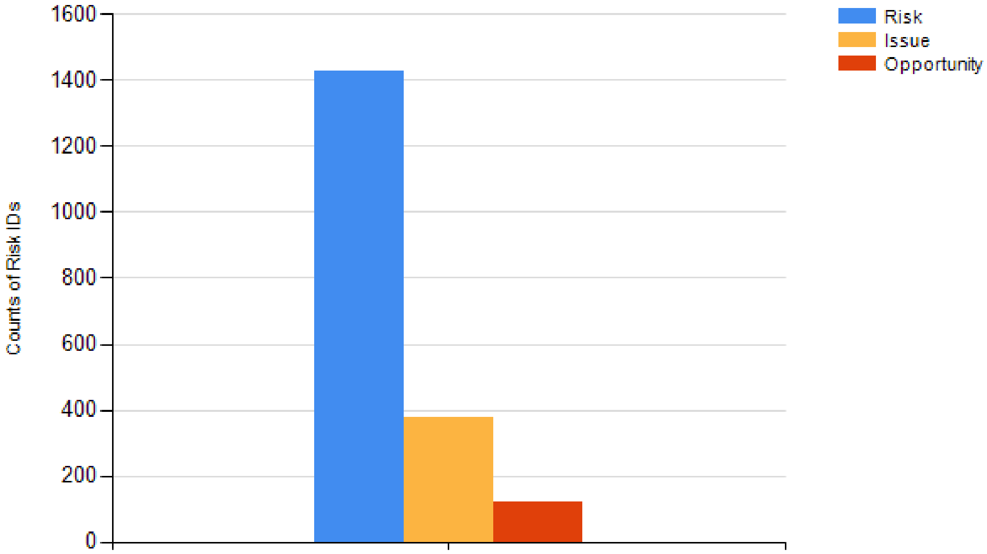


Figure 2 Risks, Issues, and Opportunities

The concept of using the difference between inherent and target risk assessments to gauge risk tolerance is not a measurement, and we needed to turn this concept into numbers and particularly, numbers that would be meaningful and easily understood.

We began by defining those differences:

- We defined a **Risk Rating Delta (RRD)** as the difference between the Inherent Risk Rating (IRR) and the Target Risk Rating (TRR) (**RRD = IRR – TRR**), where the IRR and the TRR are numeric values one (1) through 25, taken from the threat side of the PID for threat risk assessments.

- We also defined an **Opportunity Rating Delta (ORD)** as the difference between the Inherent Opportunity Rating (IOR) and the Target Opportunity Rating (TOR) (**ORD = IOR – TOR**), where IOR and the TOR are numeric values one (1) through negative 25, taken from the opportunity side of the PID for opportunity risk assessments.

Conveniently, both RRDs and ORDs turn out to be positive numbers. Not so conveniently, they do not trend from better to worse in the same direction. To solve this problem and provide meaning for risk tolerance levels, we defined five levels for threats (risks) and opportunities (rewards) as show below in Table 2 and Table 3.

Table 2 Risk Tolerance Levels

Risk Tolerance Level	Definition
5: Bold	Courageous; Daring
4: Forward-Leaning	Progressive; Aggressive
3: Moderate	Average; Less Extreme
2: Cautious	Play it Safe; Judicious with Risk Antipathy
1: Averse	Unwilling and Opposed to Take Risk

Table 3 Reward Tolerance Levels

Reward Tolerance Level	Definition
5: Exceptional	Unprecedented; Excellent
4: Significant	Serious Gain; Noteworthy
3: Moderate	Conservative; Average
2: Minor	Not Serious; Small and Unimportant
1: Negligible	Trivial; Not Noteworthy

Next, we assigned RRD and ORD value ranges to each risk tolerance level as shown below in Table 4 and Table 5.

Table 4 Risk Rating Deltas Assigned to Risk Tolerance Levels

Risk Tolerance Level	Risk Rating Delta (RRD)
5: Bold	0-5
4: Forward-Leaning	6-10
3: Moderate	11-15
2: Cautious	16-20
1: Averse	21-24

Table 5 Opportunity Rating Deltas Assigned to Reward Tolerance Levels

Reward Tolerance Level	Opportunity Rating Delta (ORD)
5: Exceptional	21-24
4: Significant	16-20
3: Moderate	11-15
2: Minor	6-10
1: Negligible	1-5

Finally, we designed two graphics to enable broader acceptance and implementation. The first, called the **Risk Reward Ratio (R3)** (see Figure 3 below), plots the organization's intersection point of current threat and opportunity tolerance on a Cartesian grid. The current R3 can be determined from existing risk data using the technique described previously. The ratio in the title reflects the values from the Risk and Reward Tolerance axes. The chart includes a second intersection point representing the organization's desired R3, which is a goal for threat and opportunity tolerance. An arrow connects the points. Over time, we expect to see the current R3 to move closer to the desired R3 as the organization risk tolerance changes.

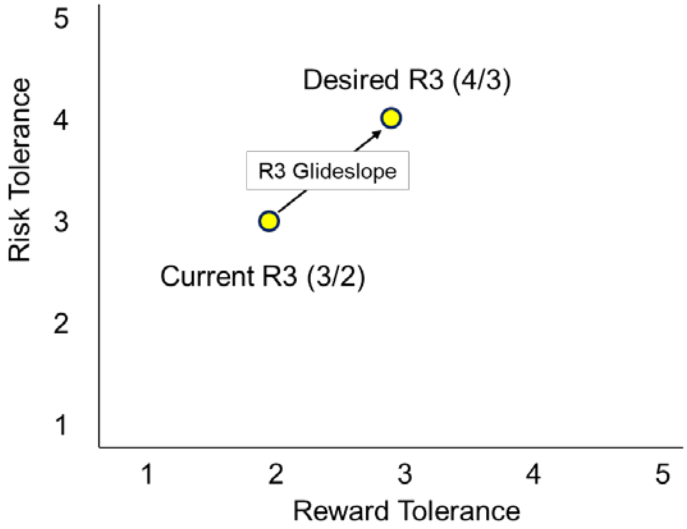


Figure 3: Risk-Reward Ratio (R3)

A second chart known as the **Risk-Reward Ratio (R3) Summation** depicts the current R3s for all the programs in a portfolio (the yellow points) in relation to the organization's overall portfolio desired R3, represented by the green point. Again, over time we expect to see the current R3s move closer to the desired R3 if the organization's overall risk tolerance is changing. This chart can also serve to represent portfolios in an enterprise.

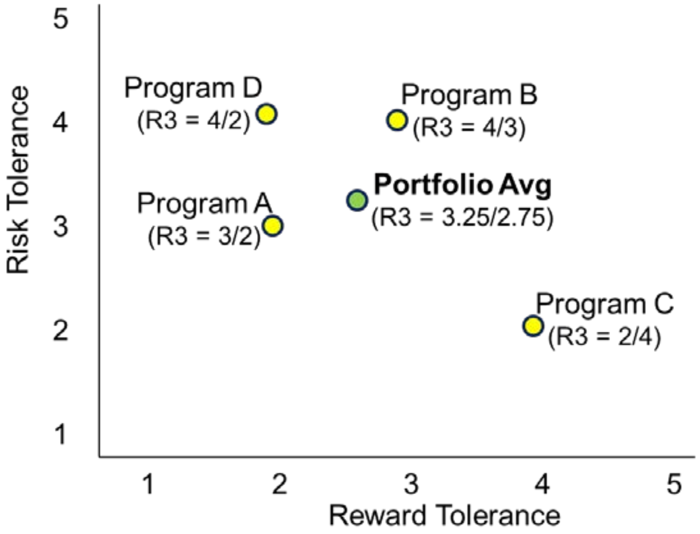


Figure 4: Risk-Reward Ratio (R3) Summation

We also developed custom reports in the CBP enterprise risk management tool to manage and present relevant calculations and translations, although it is also possible to produce the same results with an Excel workbook or a SharePoint list and view.

Changing Culture by Changing Minds

“The fastest way to succeed is to double your failure rate,” Thomas Watson, CEO, IBM.

Culture change is challenging, and most do not like to fail. Yet innovative organizations know that failure is a prerequisite to invention[25]. Changing a culture means changing minds, starting from the top and supporting change all the way to the bottom. In parallel with measures and representations, we addressed the “soft” goals of the strategy: Process; Training; Rewards and Awards; Outreach; Communications; and Policy.

Process: Risk management is a journey, not a destination,[26] and it requires the same continuous attention as any other element of management. However, risk management can consume resources long past the point of diminishing returns. Risk intolerance drives organizations to attempt the impossible: Reduce the potential impacts of uncertain future events and conditions to near zero. Unrealistic optimism, poor planning and other factors drive organizations to continue to pursue opportunities after the need is gone, or the likelihood of success is all but erased. The risk management highway

[25] Richard Farson and Ralph Keyes. August 2002. “The Failure-Tolerant Leader”. *Harvard Business Review.* https://hbr.org/archive-toc/BR0208.

[26] Kevin W. Knight. 2010. “Risk Management – A Journey, Not a Destination”. A presentation to the RusRisk/ Marsh Seminar, Moscow on 15 December 2010. https://www.scribd.com/document/283750131/A-Journey-Not-a-Destination-pdf

needs off-ramps. As the CBP Component Acquisition Executive succinctly stated, any risk management process that attempts to shift resources from threat mitigation to opportunity promotion will need to follow the guideline “fail fast and cheap.” The ART process we developed (loosely modeled after established agile software development processes) provides checkpoints as ‘off-ramps,’ as well as the ability to ‘on-ramp’ within the process, to enable rapid and continual improvement. This process depicted in Figure 5 is the key to answering the two DAU risk recommendations.

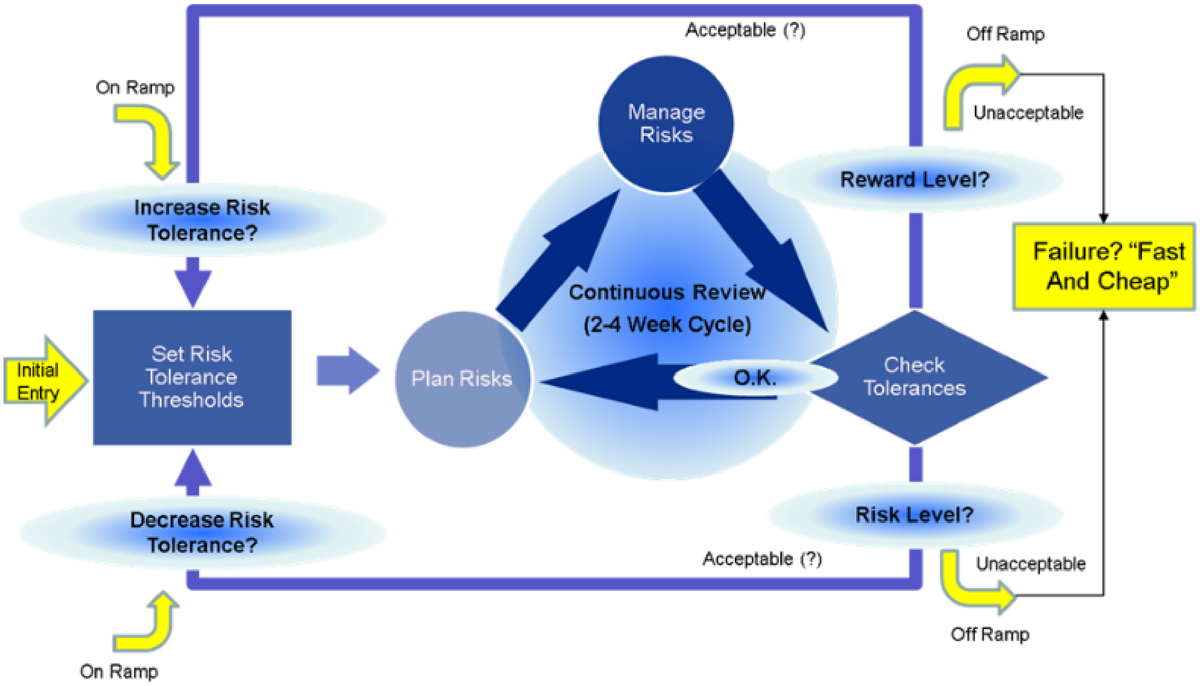


Figure 5: An ART Process

Training. For several years prior to the DAU study and the initiatives it spawned, one member of the team had regularly presented “lunch ‘n learn” continuous learning seminars and workshops on a variety of risk management subjects. This learning cycle and forum provided a natural opportunity for addressing the ART strategy’s training goals. Since January 2018, we have conducted 24 seminars to introduce and reinforce ART principles and practices. These monthly workshops are useful, but they are not a targeted delivery system. So in 2020, we began scheduling introductory presentations with specific groups, with the goal of reaching all CBP acquisition organizations before the end of the year.

Awards and Rewards. To encourage acquisition professionals to adopt risk tolerance principles and practices, we developed incentive programs that reward embracing risk tolerance in CBP programs. This addresses the second of the DAU risk recommendations of rewarding innovation. Each organization is encouraged to build such rewards into their traditional reward and recognition practices and traditions. People can receive both “On the Spot” awards from their supervisors, as well as committee-evaluated awards (i.e., Joint Awards Committee (JAC) awards). Programs can also receive “savings carry-over” awards based on quantifiable savings realized through risk tolerance practices.

Outreach. After the ART Directive was officially promulgated throughout CBP, we began outreach to program offices using targeted training, assisting them in the preparation for acquisition portfolio reviews, and collecting metrics to gauge their success in not only meeting but exceeding schedules and reducing cost. To date, we delivered training to over 350 Agency personnel in the ART method.

Communication. Continuous communications with leadership and the workforce as an enabling function in the slow process of culture change. This important component of the strategy follows the wisdom of the old proverb, “The drop does not carve the stone with force but with the steady dripping” or in the Latin version “Gutta cavat lapidem non vi sed saepe cadendum.” In this spirit we published ART articles in various newsletters and office publications and intend to continue to do so, as well as reporting on ART metrics and successes.

Policy. Formally setting expectations may not be the last step, but it is an important step. The team authored a CBP-level Directive in late 2018, signed by the CBP Chief Acquisition Executive (CAE), the Chief Information Officer (CIO), and the Head Contracting Authority (HCA). It established that “... all offices and organizations shall integrate an ART process... into their acquisition management practices and procedures[27].” Since then Agency acquisition portfolio reviews, which occur roughly every six months and include approximately ten percent of the active acquisition programs and projects, have required presenters to report on current and desired risk and reward tolerance levels. This Directive also established the position of CBP Chief Risk Officer (CRO), charged with the overall responsibility of leading the ART initiative within the Agency.

Conclusion

We have completed over two years of ART formation, introduction, and use within CBP. During this time, CBP has published an implementing directive, established and continued ART training, established relevant ART metrics, and has begun tracking metrics on a quarterly basis. We see tangible evidence that CBP ART principles and practices are taking hold in risk management plans and portfolio reviews. Our declared intent, as supported by our Agency leadership, is to focus on increasing innovation and acquisition efficiency and effectiveness. As we all know, cultural change takes time; however, the CBP ART Team is confident that with the foundation established, ART

[27] Office of Acquisition. October 2018. Directive 5220-045 “Agile Risk Tolerance”. Department of Homeland Security/ Customs and Border Protection.

principles and practices will help in achieving our Agency acquisition and procurement goals.

Bibliography

DARPA. 2020. “Budget”. Last modified March 2019. https://www.darpa.mil/about-us/budget.

Defense Acquisition University. 2015. Outbrief - Review of Customs and Border Protection (CBP) Acquisition Program...

Farson, Richard, and Keyes, Ralph. August 2002. “The Failure-Tolerant Leader”. *Harvard Business Review.* https://hbr.org/archive-toc/BR0208.

Funk and Wagnalls. 1963. *Standard College Dictionary.* New York: Funk and Wagnalls Company.

International Standards Organization. 2009. *Guide 73 Risk management – Vocabulary.*

Knight, Kevin W. 2010. “Risk Management – A Journey, Not a Destination”. A presentation to the Rus/Risk Marsh Seminar, Moscow on 15 December 2010. https://www.scribd.com/document/283750131/A-Journey-Not-a-Destination-pdf

NASA. 2020. “NASA Budget, Current Funding, History, and Economic Impact”. Last modified February 27th. https://www.thebalance.com/nasa-budget-current-funding-and-history-3306321.

Office of Acquisition. October 2018. Directive 5220-045 “Agile Risk Tolerance”. Department of Homeland Security/ Customs and Border Protection.

The Committee of the Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management – Integrated Framework. Executive Summary – Framework.*

U.S. Department of Defense, Government Services Agency and National Aeronautics and Space Agency. 2020. *Federal Acquisition Regulations.* Washington, D.C.

About the Authors

Marty G. Meyer is the Chief Engineer and CRO for CBP. He is a retired U.S. Air Force officer and served in numerous operational, engineering and program management positions prior to joining CBP. Mr. Meyer received a B.S. in Civil Engineering from the U.S. Air Force Academy and a MBA from Golden Gate University.

Dr. Gunter Brunhart is a nuclear physicist who joined the CBP SBInet program in 2007 serving in various positions in the Systems Engineering Directorate of the Office of Acquisition as Technical Director and Branch Chief for Engineering Management including Risk Management. Previously, he spent many years in basic nuclear research, biomedical radiation research, and Navy survivable communication in nuclear war scenarios.

Dr. Steven Moyer serves as Deputy Chief Engineer and Deputy CRO for CBP. Previously, he worked at the U.S. Army Night Vision and Electronic Sensors Directorate (NVESD) in the Modeling and Simulation (M&S) Division. He received a Ph.D. from the Georgia Institute of Technology and an M.S. in Optics and a B.S. in Electrical Engineering from the Pennsylvania State University.

Dr. Richard Dubs serves as a subject matter expert in the Workforce and Knowledge Management Division of OA where he develops tools for analyzing and predicting acquisition workforce needs across CBP programs. He also helps develop “Career Path Models” for the various CBP acquisition disciplines. Dr. Dubs received a Ph.D. from the California Institute of Technology and a B.S. from Union College.

Mr. Thomas Erickson serves as a support contractor to the Chief Engineer and CRO for CBP and as a support contractor to all CBP offices for matters related to risk management. He is a retired Air Force acquisition officer and holds a B.S. in Electronic Engineering (Circuit Design) from Minnesota and an M.S. in Engineering Management from George Washington University. He is also a registered Professional Engineer in Electrical Engineering and is credentialed by the Program Management Institute as a Program Management Professional (PgMP).

Mr. Robert Skalamera serves as a support contractor to the Chief Engineer and CRO for CBP. Previously, he retired from the Senior Executive Service having served as Director for Systems Engineering Policy in the Office of the Secretary of Defense. Mr. Skalamera has a M.S. in Computer Engineering from the Pennsylvania State University and a B.S. in Electrical Engineering from Drexel University.

Mr. Rob Kepner is a registered professional engineer and acquisition system engineering professional with the MITRE Corporation supporting CBP’s Chief Engineer and CRO. Previously, he supported numerous federal clients in establishing acquisition polices, practices, and program management and systems engineering offices. Mr. Kepner has a M.S. in Mechanical Engineering from the Catholic University and a B.S. from Virginia Tech.

tfc
CELEBRATING 15 YEARS OF EXCELLENCE
Every move is strategic.
PERFORMANCE
VALUES
OUTCOMES
ASK US HOW WE CAN HELP YOU IMPROVE YOUR PERFORMANCE
We Listen | We Innovate | We Deliver
240.453.6288
ddatskovska@tfcci.net
tfcci.net

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.

There are 37 separate conversations on ERM on the website. Here are the five most recent discussion topics with active links to each:

- Private sector businesses often play a balancing act between company profit and insolvency risk. Is it necessary to perform similar analysis as part of a public sector ERM program, and how would that analysis differ?
- How does the application of ERM differ in making risk mitigation decisions vs. routine decision making?
- What methods can agencies use to identify risks that are not already realized problems?
- What are some of the top challenges facing agencies in integrating the OMB A-123 ERM framework with strategic objectives and decision-making processes?
- How can the agency ERM process and risk appetite principles be used to assist in mitigating strategic (long-term) risks resulting from COVID-19?

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

AFERM
Association for Federal
Enterprise Risk Management

AFERM Newsletter

Issue 35
December 2020

Thought Leadership for the Federal Enterprise Risk Management Community

AFERM's Communities of Interest/Practice

Supporting Federal ERM areas of specialty

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

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

Thought Leadership

ERM and third-party service providers

By Ed Hau, Director, ASR Analytics, and Harold Barnshaw, Director of Accounting, Office of the Comptroller of the Currency

What follows is a mock discussion between an executive at a federal agency (“Sam”) and a former Big 4 risk advisory partner now working as a director at a DC metro area management consulting firm (“Wynn”). This encounter takes place at a coffee shop with facial coverings and appropriate social distancing.

Wynn: It’s good to see you out and about. As we head into 2021, what is on your mind other than COVID-19?

Sam: Believe it or not, third-party service providers to the federal government. This past fiscal year, we ran into trouble with one of our major service providers. Everything turned out all right. We still earned a clean financial statement audit opinion, but it got me thinking about enterprise risk management, or ERM as it’s known in the industry, and the impact third-party service providers have on our agency’s ERM risk profile.

Wynn: How so?

Sam: Well, ERM at its heart is about identifying, assessing, prioritizing, and mitigating business risks. In the context of business goals and strategies, you analyze key risks and current capabilities. It helps you determine where to focus your limited attention and resources. I am just not sure how to effectively detect emerging risks promptly when it comes to third-party service providers.

Wynn: Tell me more about your experience with third-party service providers and the related risks. What risks have emerged and how have you achieved internal control coverage?

Sam: We receive Statement on Standards for Attestation Engagements No. 18 reports, or SSAE 18s, each year from our third-party service providers. It’s a key piece of support relied upon by management and our external financial statement auditors.

The problem this past year was that one of the SSAE 18 reports was released by the service auditors weeks later than usual, and too late for our financial statement auditors to consider it. To compound matters, the SSAE 18 report contained an adverse opinion from the service auditors. Needless to say, this caused quite a flurry of activity within our agency. Nonetheless, it turned out to be a non-issue as our agency was able to provide adequate control evidence and other supporting documentation to our external auditors that the controls we had in place were sufficient and effective to identify any material issues with the transactions interfaced from the service provider into our financial systems.

Wynn: That's good because your third-party service providers are part of your extended enterprise. If they have a problem, you have a potential problem. Unfortunately, most organizations think they are reducing or eliminating their ERM risks by transferring them to a service organization to fully manage.

Sam: That's what scares me. We thought we had done everything right in terms of internal controls coverage – both by relying upon support from this third-party service provider and by maintaining our own complementary user entity controls or CUECs. Nonetheless, the late release date of the SSAE 18 report, coupled with the unexpected results, gave us little time to react to our financial reporting risks and identify compensating controls. Our internal controls and CUECs proved to be sufficient and financial reporting was not at risk, but it could have been.

Wynn: You certainly found yourself in a tough spot. It's hard to achieve a clean financial statement audit opinion without effective controls at third-party service providers. And, if service provider organization controls break down, you as the customer organization need to remain vigilant and ready to react to address your financial reporting risks. Just when you thought your ERM risks, including those related to financial reporting, were mitigated or reduced by transferring them to the service organization, residual risks quickly boomeranged back to your organization.

Sam: Do you have any advice on how to anticipate and lower the risk that something will go wrong with a third-party service provider?

Wynn: The most important thing is to set clear service level expectations up front with each of your service providers. You should demand that as the customer. In many cases, you will have options to take your business elsewhere if your expectations are not met by the service provider. You also have to have robust ERM assessment and monitoring practices. There should be no confusion about how you are going to evidence the key controls you are relying on at the service provider are properly designed and operating effectively.

Receiving an SSAE 18 report, assuming an appropriate scope and a clean audit opinion, is one way to achieve that coverage. You should also make sure to routinely revisit your CUECs to make sure that you have coverage per your third-party service provider agreement and that they are also properly designed and operating effectively.

Sam: That's helpful information. We strive to make appropriate decisions about risk and adjust those decisions on the basis of new information. We will continue to monitor our third-party service providers closely and review the status of our compensating customer organization internal controls. If necessary, we can always look into moving to a new service provider.

Wynn: While moving to a new service provider should be an option in many cases, it is often easier said than done at a federal agency; especially if every other component agency within your Department uses that same provider.

Sam: I think I'll take your advice and revisit the service level expectations across all of our service providers. Where we do rely on SSAE 18 reports for some control coverage, I will also make sure that we have all of the necessary CUECs designed, in place, and operating effectively. I'll also look into the extent to which my organization has compensating controls that could be relied upon in the event of future SSAE 18 reporting issues.

Wynn: This reminds me of COVID-19. If you have the virus, you can transmit it up to two weeks before you show symptoms. You can also have problems at a third-party service provider long before you receive the SSAE 18 report.

Sam: True, but the country is rolling out the vaccine quickly now. I have high hopes for 2021. Have a great day.

Wynn: I look forward to speaking with you again.

Ed Hau may be reached at Ed.Hau@asranalytics.com, and **Harold Barnshaw** may be reached at Harold.Barnshaw@occ.treas.gov.

No open season needed
Life insurance on your time.
Visit waepa.org
WAEPA
Group Term Life Insurance
Serving Civilian Federal Employees Since 1943

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.

2021 AFERM Officers

President

Nicole Puri

Past-President

Ken Fletcher

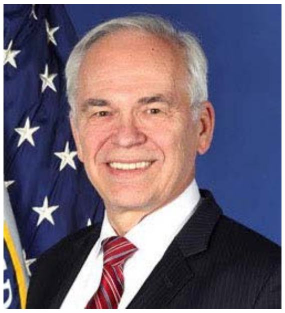
President Elect

Daniella Datskovska

Secretary

Thomas Holland

Treasurer



Doug Webster

Vice President at Large

Harold Barnshaw

Vice President at Large

Curtis McNeil

Vice President at Large

Alice Miller

AFERM
Association for Federal Enterprise Risk Management

AFERM Newsletter

Issue 35
December 2020

Thought Leadership for the Federal Enterprise Risk Management Community

2021 AFERM Committees and Communities

Audit
Alex Ng, Chair

Communications
Shelly Turner, Chair
Nadya Korobko

Finance/Budget
Doug Webster, Chair

Infrastructure and Operations
Ed Hau, Chair

Knowledge Capital
Brian Murphy, Chair
Tim Weber

Membership
Yehuda Schmidt, Chair
Domenyck Schweyer

Outreach and Advancement
Curtis McNeil, Chair
Cynthia Vitters, RIMS Liaison

Planning
Christine Girardi, Chair
Marc Pratta, Co-chair

Programs
Varun Malhotra, Chair

Summit 2021 Planning
Marianne Roth, Co-chair
Mike Batlogg, Co-chair

Volunteers
Irena Marchand, Chair
Janice Ho, Co-chair

Cyber ERM Community of Interest
Nahla Ivy, Chair
Julie Chua, Co-chair

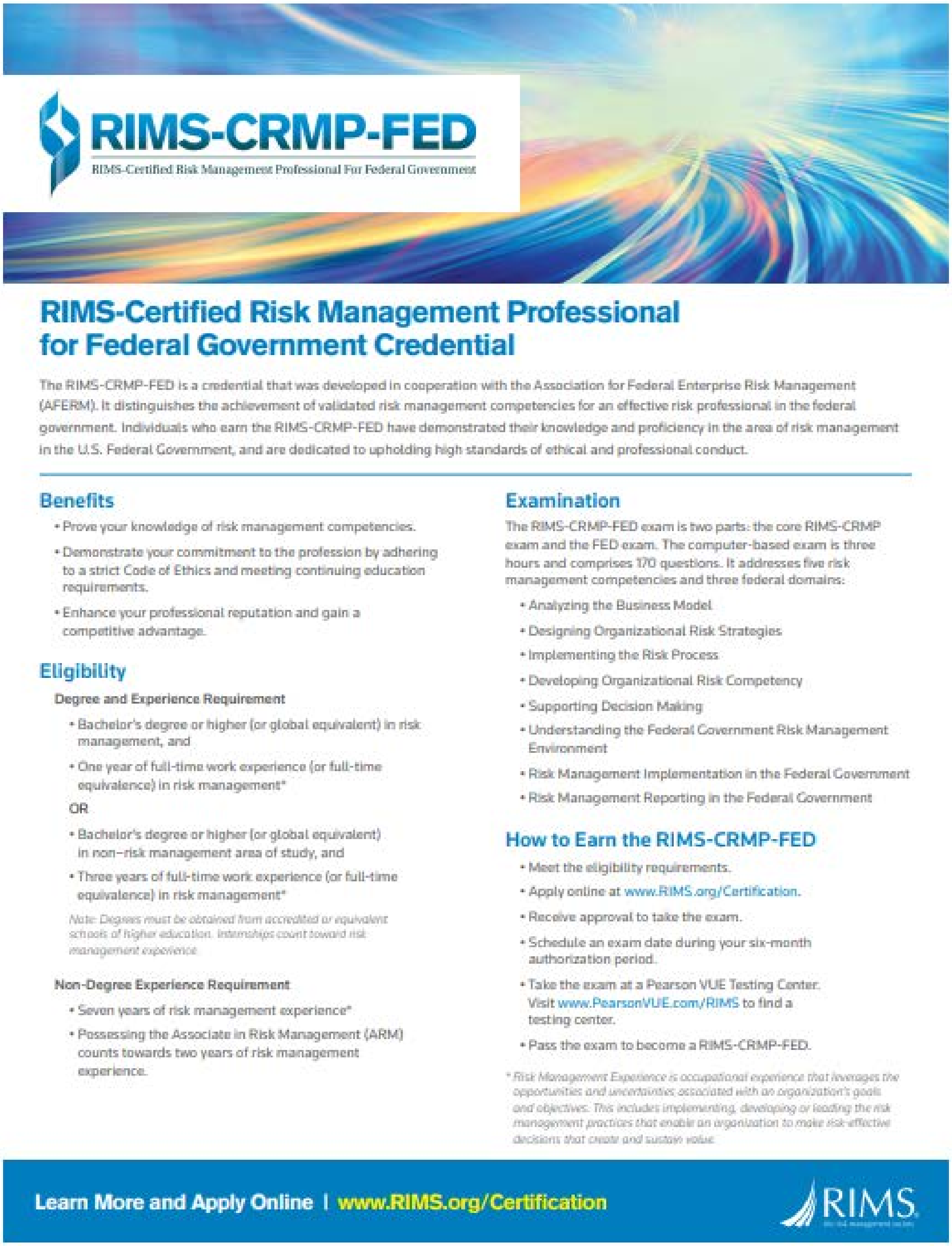
Data Analytics Community of Practice
Curtis McNeil, Chair

Small Agency Community of Practice
Marianne Roth, Chair
Tal Seaman, Co-chair

Corporate and Associate Advisory Group (CAAG)
Platinum Sponsors
Sean Vineyard, 11th Hour Service
Cynthia Vitters, Deloitte LLP
Chris Hare, Ernst & Young
David Fisher, GuideHouse
David Zavada, Kearney & Company
Tim Comello, KPMG LLP
Carrie Everett-Vaughn, RSA
Gold Sponsors
Bobbie-Jo Pankaj, Grant Thornton
Silver Sponsors
Simone Reba, Accenture Federal
Jeannine Rogers, AOC Solutions
Stephanie Irby, BDO
Bert Nuehring, Crowe LLP
Jack Downes, Elevate Government Solutions
Jillian Campbell, Galvanize
Tim Mobley, IRIS Intelligence
George Fallon, RMA Associates, LLC
Sim Segal, SimErgy Consulting
Tashu Trivedi, TFC Consulting, Inc.
Paul Marshall, The MIL Corp
Celine Serrano, WAEPA
Jay Colavita, Workiva/Vertosoft

CAAG Liaison
Sarah Choi

RIMS-CRMP-FED Certification



RIMS-CRMP-FED

RIMS-Certified Risk Management Professional For Federal Government

RIMS-Certified Risk Management Professional for Federal Government Credential

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

Benefits

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

Eligibility

Degree and Experience Requirement

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

OR

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

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

Non-Degree Experience Requirement

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

Examination

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

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

How to Earn the RIMS-CRMP-FED

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

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

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

RIMS

Corporate Sponsors and Partners

Thank you for your support!

Platinum Sponsors

11TH HOUR SERVICE

Deloitte.

EY Building a better working world

Guidehouse

KEARNEY& COMPANY

KPMG

RSA

Gold Sponsors

GrantThornton

Silver Sponsors

accenture

AOC SOLUTIONS

BDO

Crowe

elvt-govt elevate government solutions

Galvanize

IRIS INTELLIGENCE

MIL corp.

RMA Associates
Auditors. Consultants. Advisors.

simergy
THE ERM SPECIALISTS

tfc

WAEPA

wdesk

Educational Development and Community Partners

GW

RIMS
the risk management society™

SENIOR EXECUTIVES ASSOCIATION

NGMA
National Grants Management Association