

Thought Leadership for the Federal Enterprise Risk Management Community

Table of Contents

President's Corner 2

Spring Risk Podcasts..... 3

ERM Educational Events 4

Operational Risk Management..... 5

Leveraging Audit Reports as a Risk Management Tool ... 8

Key Considerations for Technology Enablement of ERM . 9

Audit Tips & Tricks..... 15

Corporate Sponsors 16



Disclaimer

This issue of the AFERM Newsletter includes two sponsor created thought leadership articles from ERM practitioners. Please note that, views expressed in those articles are those of the authors only, and do not necessarily reflect the views of AFERM.

President's Corner

By: Marianne Roth, AFERM President



Greetings AFERM Members and Sponsors! Although my term as President began in November, this is my first opportunity to highlight AFERM's accomplishments and upcoming initiatives and events in the revamped AFERM Newsletter. I want to thank Montrice Yakimov, Vice President of Communications and Outreach and Laura Gray, Communications Committee Chair for all their hard work in redesigning the newsletter to better meet the needs and interests of AFERM Members.

It's hard to believe we're halfway through 2023! We've been focused on continuing to advance the practice of ERM by delivering top-notch trainings, creating opportunities for networking and professional development, and sharing lessons learned and thought leadership. In April, more than 60 federal ERM practitioners attended the annual ERM Workshop co-sponsored by AFERM and AGA. We were thrilled to conduct the workshop in person this year and attendees were able to engage in small group, facilitated table discussions, and share "how-to" explanations and examples. In May, we launched the first ERM Book Club under the outstanding leadership of Melissa Thomson, State and Local Outreach Committee Chair. Personally, I really enjoyed the session and loved hearing directly from the authors. We've continued to air Risk Chats, providing insight into the approaches many of our colleagues took in implementing ERM across a range of agencies and touching on promising practices, lessons learned, and helpful experiences from which we all can gain. Finally, the Small Agency Community of Practice (SACoP) hosted its first in-person happy hour in March. It was so much fun to re-connect with colleagues in person. I hope you can join us at the June SACoP Happy Hour. Details to come!

We are excited to have begun preparing for the AFERM marquee event – our annual Summit. I would like to personally thank Bobbi-Jo Pankaj and Melissa Reynard, Summit Chair and Co-Chair, for leading the Summit planning. We are thrilled to announce the Summit will be held at the Walter E. Washington Convention Center on November 28 and 29, 2023. Please be on the lookout for early bird registration announcements. Additionally, there is still time to volunteer on a committee to help shape the Summit's plenary and breakout sessions, as well as aid with marketing and logistics.

We plan to offer more events leading up to the Summit, including bringing back the in-person ERM Luncheons, so please keep an eye on our announcements. AFERM's Programs Committee, led by Alyssa Fusisi of Kearney & Company is lining up a series of webinars and events on topics that align with the challenges and opportunities facing your organization, including cyber security, organizational resiliency, and more.

Thought Leadership for the Federal Enterprise Risk Management Community

Lastly, I am honored to serve as President of an organization that offers abundant opportunities to learn and share ERM knowledge, influences governmental risk management policies and practices, advocates for the ERM profession, and brings together ERM practitioners to meet, network, and socialize with colleagues across the country. I'm always interested in learning how we can better serve our members, so feel free to email me at president@aferm.org with your questions and concerns. I look forward to seeing a lot of you in the coming weeks and months, especially at the 16th Annual ERM Summit in November!

Best,
Marianne

Spring Risk Podcasts

Interested in Current Risk Chats? Check out the May [AFERM Podcasts](#):

Elizabeth DeVoss, Chief Financial Officer at Health Resources and Services Administration (HRSA) and Cynthia R. Baugh Associate Administrator/ Chief Grants Management Officer at HRSA sat down with AFERM to discuss HRSA's budget, financial policy and grant oversight efforts that integrate ERM into HRSA's internal controls processes. Some highlights include:

- COVID pandemic's impact on HRSA's grants management operations and systems
- Discussion on the value of strong internal controls, collaborative partnerships; and a history of sound policies/process that support its ERM approach.

The Environmental Protection Agency's (EPA's) Nikki Wood and Bradley Grams chatted about EPA's approach to ERM!

AFERM's State and Local Outreach Committee Chair Melissa Thomson discussed the City of Phoenix's ERM program and the unique challenges of establishing a program at a large city.

[> Listen to these podcasts & more](#)

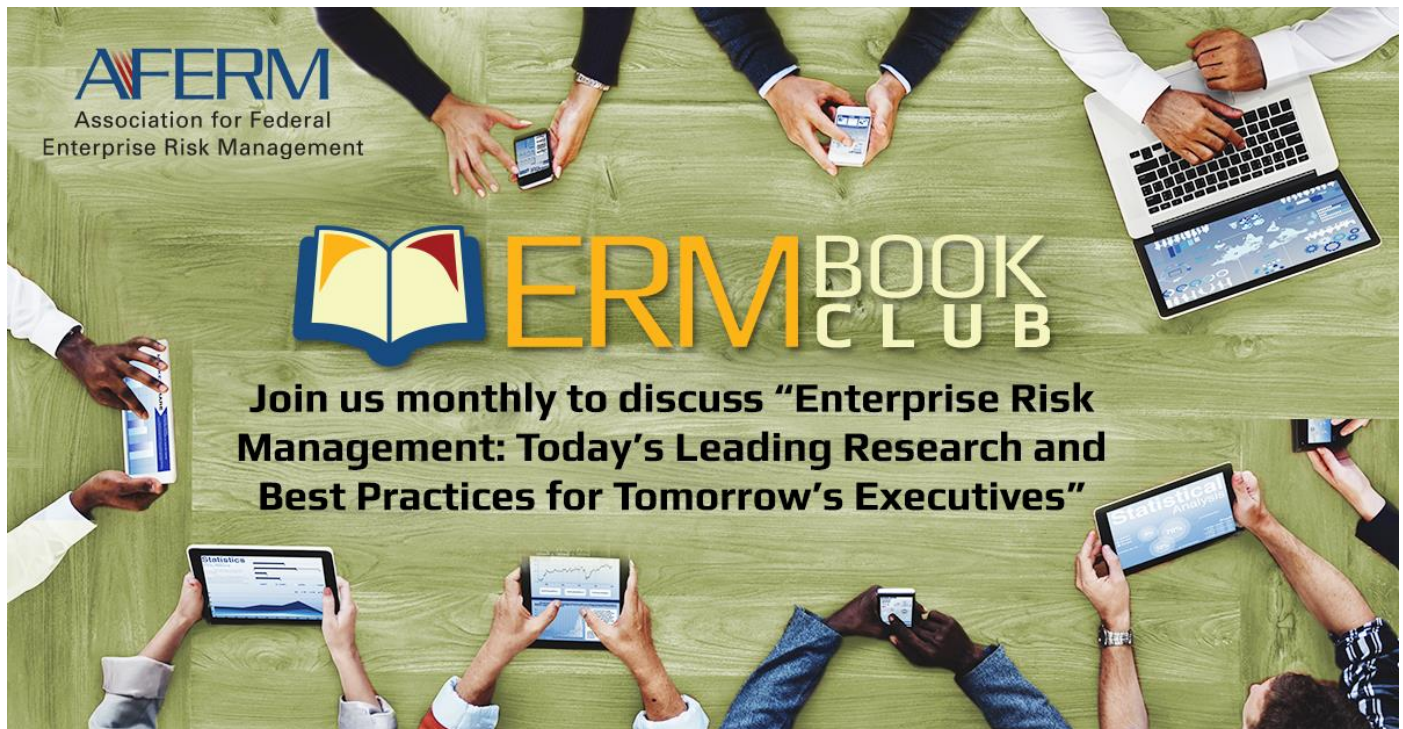
ERM Educational Events

Discuss ERM tools and templates at these [upcoming educational events](#)

- [GW: Enterprise Risk Management Mini Boot Camp](#) — June 6, 2023
- [GSA: Contract Specialist Virtual Career Fair](#) — June 6, 2023
- [SimErgy: June 2023 ERM Boot Camp Online Event](#) — June 20-21, 2023
- [Performance Institute: Government Performance Summit 2023 \(GPS23\)](#) — June 20-21, 2023
- [AFERM Book Club](#) — June 22, 2023, and Ongoing Monthly

Please visit our website for more information at aferm.org/events-list.

Alyssa Fusisi of Kearney and Company is the AFERM Programs Committee Chair. They may be contacted at Programs@AFERM.org.



The graphic features a top-down view of several people's hands and forearms gathered around a light green wooden table. Some hands are holding smartphones, others are using laptops or tablets. In the top left corner, the AFERM logo is displayed with the text 'Association for Federal Enterprise Risk Management'. In the center, there is a stylized icon of an open book with yellow and red pages, followed by the text 'ERM BOOK CLUB' in large, bold, yellow and white letters. Below this, a black text box contains the invitation: 'Join us monthly to discuss "Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives"'. The overall theme is professional collaboration and learning.

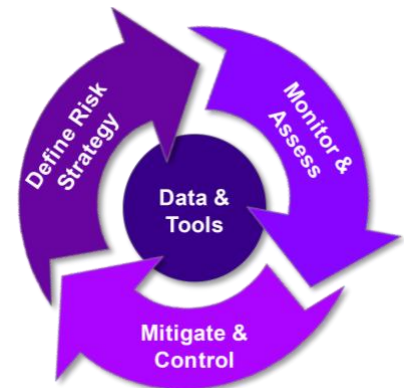
Operational Risk Management

By: Dan McGuinn, Dan Featherly and Jordan Michalak; Accenture

Operational risk is inherent in all federal agency activities, processes, and systems, and the effective management of operational risk is a fundamental element of any agency’s risk management program. At its core, operational risk is the risk of loss resulting from inadequate or failed internal processes, technology, even people, or from external events, which would impact the mission. Agencies need an effective Enterprise Risk Management (ERM) program to proactively identify risks to mission objectives, measure exposures to those risks, and ensure that an effective monitoring program is in place. As Figure 1 illustrates, effective risk management has multiple phases.

The four key principles in Figure 1 underpin an effective operational risk framework and guide organizations to better manage enterprise and operational risk:

1. Define Risk Strategy to articulate risk appetite within a business context. This includes determining the level and types of operational risks the organization is willing to accept to achieve desired mission outcomes.
2. Monitor & Assess point in time and forward-looking operational risk exposure and ensure appropriate processes are in place to support targeted analysis.
3. Mitigate Risk & Control against operational risk breaches, including effective management of heightened risk and actions to bring the organization back within risk appetite.
4. Leverage data & tools to support risk identification, management, and reporting. Data should be actionable and support the entire operational risk framework for effective decision-making.



Define a Risk Strategy

An effective risk management operating model helps in managing an agency’s overall governance and compliance functions. A structured approach helps align mission objectives while effectively meeting compliance demands and managing risks. The goal of this strategy is to move toward a fully integrated ERM program that proactively manages risks in a holistic framework, as shown in Figure 2.



Figure 2: Holistic Operational Risk Management Strategy

Thought Leadership for the Federal Enterprise Risk Management Community

Two key aspects of an effective operational risk management strategy are risk appetite and risk tolerance. Although these terms are used interchangeably, there are nuances between the two that are important to understand.

Risk tolerance is the amount of uncertainty an agency is prepared to accept in total or more narrowly within a certain program or initiative. Expressed in quantitative terms, risk tolerance often is communicated in terms of acceptable or unacceptable outcomes or as limited levels of risk. Risk tolerance statements identify the specific minimum and maximum levels beyond which the organization is unwilling to lose. Exceeding the organization’s established risk tolerance level not only may imperil its overall strategy and objectives, but also its very survival.

Risk appetite is the total exposed amount that an organization wishes to undertake based on risk-return trade-offs for one or more desired and expected outcomes. As such, risk appetite is inextricably linked with, and may vary according to, expected returns. Risk appetite statements may be expressed qualitatively and/or quantitatively and managed with respect to either an allocated individual initiative and/or in the aggregate. Think of risk appetite as the amount that an organization actively ventures in pursuit of its goals and objectives.

Monitor and Assess

Once the risk management strategy is defined, based on the agency’s mission and strategy, it is critical to implement a risk assessment framework that translates to people, processes, and technology. Figure 3 below shows leading practices and recommendations for implementing your operational risk management strategy and accurately assessing risks.



Figure 3: Leading Practices in Operational Risk Management

Thought Leadership for the Federal Enterprise Risk Management Community

Mitigate and Control

The purpose of risk monitoring and control testing is to identify, analyze, and plan for newly discovered risks and manage identified risks.

Internal controls should be designed to provide reasonable assurance that an agency will have efficient and effective operations, safeguard its assets, produce reliable financial reports, and comply with applicable laws and regulations.

Maintaining three lines of defense is a best practice for control testing. Typically, these include the Business Control Function, Compliance & Operational Risk, and Internal Audit, explained in detail in Figure 4. Each of the three lines of defense has an important role in control testing but are most effective when there is a clear ownership of roles and responsibilities.

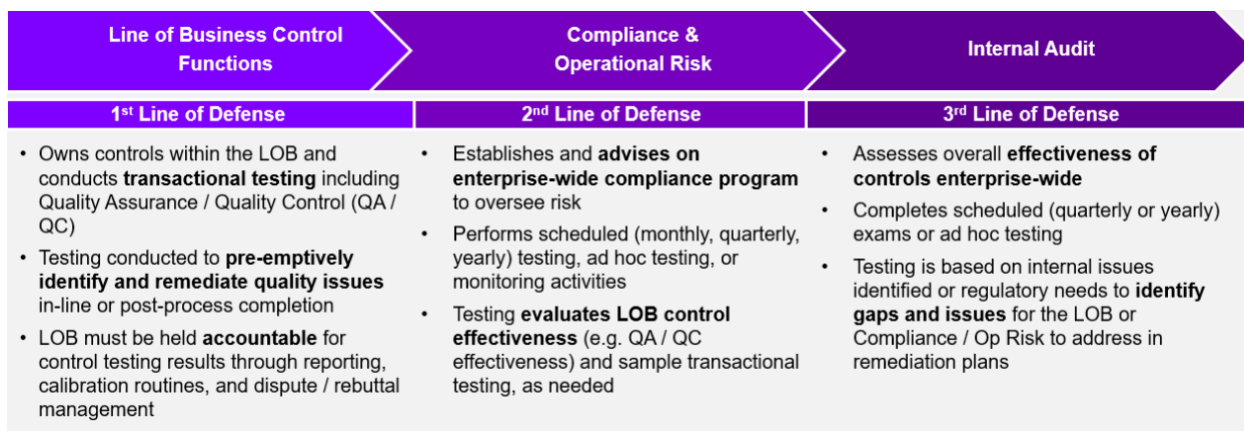


Figure 4: The Three Lines of Defense

Gain Insight for Your Risk Management Program with Data Tools

To gain efficiencies and leverage the full power of a robust operational risk management program, agencies can utilize dashboards to leverage analytics and visualizations to drive value out of data. Dashboards can integrate operational production data (task, entity level) with risk and control data (issue and quality level) across region, team, and associate to help identify high performance areas, issues, and process improvements.

Organizations should continue to evolve their analytics capabilities, shown in Figure 5, to allow for continuous monitoring across all three lines of defense.

Thought Leadership for the Federal Enterprise Risk Management Community

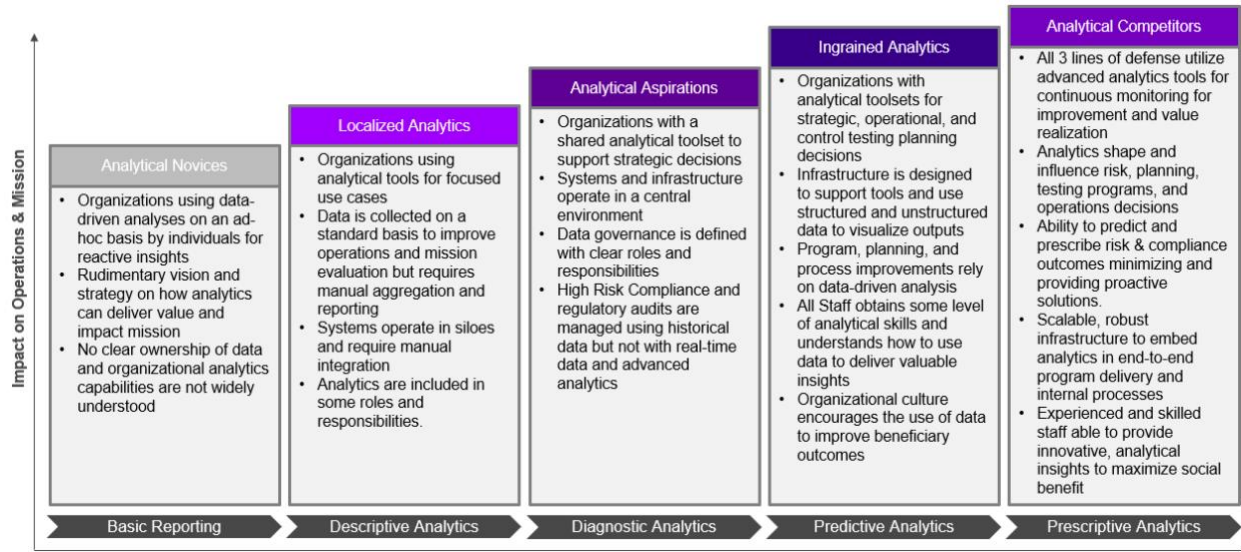


Figure 5: Leverage Data and Analytics to Support Risk Management and Achieve the Mission

Operational Risk Management is About Accomplishing the Mission

A successful operational risk management program protects the mission and helps the agency achieve its goals while proactively maintaining resilient operations. A properly integrated operational risk management program should help the agency operate more efficiently while increasing public confidence and trust. Additionally, leveraging analytics can provide a steady flow of information and a clear picture of potential risk for the agency. By gleaning data from analytics and visualizations, leadership can gain efficiencies, be proactive, and have informed decision-making that keeps the mission first.

Leveraging Audit Reports as a Risk Management Tool

By: Montrice Yakimov, Vice President of Communications and Outreach, AFERM Board

Audit reports, issued by Offices of Inspector General or the Government Accountability Office, often assess key areas of internal control such as compliance with applicable statutes, federal guidance, federal standards, and regulations. Audit reports may also highlight best practices and increasingly address how organizations should identify and mitigate risks, consistent with their risk appetite.

To leverage such helpful audit insights, risk professionals may consider searching for reports related to their organizational internal control needs. This may include compendium reports that typically summarize findings that auditors developed based on a number of audits that addressed a particular area such as [Disaster Recovery](#) or [Diversity, Equity and Inclusion](#) programs. Such reports may provide helpful food for thought when working with other leaders in an organization to plan or enhance a program or strategy. A good source of such information is the Council of the Inspectors General on Integrity and

Thought Leadership for the Federal Enterprise Risk Management Community

Efficiency ([CIGIE](#)). The CIGIE is an independent entity established within the executive branch to, among other things, address integrity, economy, and effectiveness issues that transcend individual Government agencies.

Reviewing audit reports related to a program, draft strategy, or related topic, may be helpful to identify risks that your organization should manage and mitigate. This information may help to establish the context for the risk environment. Considering questions such as the following may be helpful:

1. How applicable are the primary findings and recommendations to your organization's need?
2. Are there similar exposures, risks, or threats?
3. Is trusted data available to inform the extent to which your organization may be exposed to gaps in internal controls, compliance with applicable requirements, or other issues that resulted in auditor recommendations?
4. Have other agencies implemented a similar program, strategy, or related topic where lessons-learned may be available and helpful to your organization?
5. Would it be helpful to share potential observations from a review of audit reports that relate to your organization's need?
6. Reviewing assessments of other organizations may provide a starting point for quality risk management.

Learn more audit ready tips by viewing the [2022 AFERM Audit Ready video](#) in this newsletter!

Key Considerations for Technology Enablement of ERM

By: Soumya Chakraverty, Risk Pro Solutions LLC and Jack Downes and Kevin Schreck, Elevate

As organizations continue to navigate an ever-evolving landscape of risks and uncertainties, enterprise risk management (ERM) has become a top priority. With advances in technology, ERM can now be more sophisticated and efficient than ever before. In this article, we delve into the world of technology-enabled ERM and explore how it is transforming the way agencies approach ERM. Join us as we examine the latest trends and innovations in this critical field and discover what they mean for your organization's success.

Perspective: Is ERM technology a blessing or a curse?

The short answer is "it depends", but to thoroughly answer this question we must first make an honest assessment of the overall ERM program. While it is common to find point solutions being deployed for automation of relatively "simple" ERM programs to readily enable process automations and streamline

Thought Leadership for the Federal Enterprise Risk Management Community

program architecture, larger organizations are likely to have more complex programs that require more sophisticated solutions, which in some cases, require a mix of technology solutions. In such cases, the degree to which a single or multiple Governance, Risk and Compliance (GRC) systems can integrate different risk management activities and provide a seamless user experience, defines the success of the program and the level of user adoption. Additionally, program and process maturity is a key factor that affects the overall success of the solution. The organization, including its people, processes, systems, data, and policies must be thoroughly prepared for the adoption of technology.

Automation may not always be the right answer to drive maturity of ERM. If the size and complexity of the ERM programs and activities are such they are able to be sustained with low degree of automation then perhaps the relative value-add for the technology enablement does not justify the investment.

While selecting an ERM solution agencies should evaluate to determine which solution(s) would provide the most value in terms of meeting requirements and sustainability. Figuring out the extent to which the solution can be used to integrate various risk management functions and processes across the organization, and clearing any roadblocks for onboarding critical risk functions onto the GRC solution will contribute to greater success of the overall program.

The Role of Technology in ERM Enablement

GRC solutions have many capabilities that can enable and mature ERM. Key capabilities include:

- Centralized repository of enterprise hierarchies, processes, risks, and controls
- Risk and control self assessments (RCSA)
- Top and emerging risk assessment
- Risk aggregation
- Risk appetite metrics
- Automated controls monitoring and testing
- Risk mitigation through Issue management
- Integrated risk analytics

For the purpose of this discussion, we would like to recognize there is an overlap in the terms 'ERM,' Integrated Risk Management (IRM), and enterprise GRC or eGRC, and these terms are often used interchangeably. Technology capabilities across these three areas are generally compatible and commonly referred to as GRC or eGRC tools or solutions. As such, for the rest of the document, the term GRC will be used throughout. What is most important is to establish a common lexicon to describe the solution capabilities with the project stakeholders and use it consistently for the duration of the project.

The following table shows how GRC Technology Capabilities enable ERM Outcomes:

<u>GRC Solution Capabilities</u>	<u>ERM Outcome</u>
Enterprise Process, Risk and Control Repository	<ul style="list-style-type: none"> Establishes a repository of interconnected risks Creates shared processes and controls view and elimination of redundancy
Organizational and Process Hierarchies	<ul style="list-style-type: none"> Establishes organizational accountability for risk management activities
Risk and Control Assessments	<ul style="list-style-type: none"> Helps to integrate risk identification, assessment and management into a cohesive set of activities, prioritizes risk-based mitigation
Automated Control Monitoring and Testing	<ul style="list-style-type: none"> Facilitates the evaluation of effectiveness of risk mitigation through controls monitoring and testing Helps with proactive identification of gaps in internal controls to prevent breakdowns and disruptions
Risk Analytics and Dashboards	<ul style="list-style-type: none"> Enables Risk aggregation based on multiple dimensions (e.g. organizational hierarchy, process, product or initiative etc.) Creates alignment between risk, strategy and performance
Workflow Integration	<ul style="list-style-type: none"> Drives consistent execution of ERM processes Manages actions and notifications seamlessly between multiple stakeholders

Myth Busters about ERM/GRC Technology

We often confront assumptions about GRC technology solutions that aren't entirely true. Regardless of their origin, it is important to understand the realities associated with many of these errant assumptions. Although this summary list is by no means exhaustive, it does provide a representation of some of the more common "myths."

Myth	Reality
Implementation of technology will drive process maturity	Tools offer flexibility in configuration based on existing processes, and will not influence process changes
The solution will work "out of the box"	Configurability of a GRC solution may not be adequate to meet the process needs, requiring extensions and customizations
A single technology solution will suffice	Although you might be able to select one primary ERM/GRC platform, there are many ancillary and enabling technologies that must be considered for effective implementation and outcomes
Benefits of using technology will be realized as soon as we deploy	Until delivery is complete, more problems may be created than solved Even after deployment, benefit realization may take up to a year due to change adoption

Key Considerations & Pitfalls for Technology Enablement

Once you have committed to a GRC technology deployment to enable your ERM program, it is important to prepare as much as possible for the implementation from beginning to end. Many of the lessons learned we share here are common across all types of IT projects but they are worthy of discussion particularly for organizations that have never experienced it.

Pre-Implementation

Prior to implementing, the focus should be on establishing common ground with stakeholders and eliminating unknowns. Be sure to find a strategic leader (preferably more than one!) to champion your effort over the course of the project. As discussed earlier, a thorough understanding of requirements and objectives will enable you to begin with the end in mind and develop a plan that achieves the desired end state. Although it is important to embrace all stakeholders and extract maximum value from your project, don't be afraid to kill the good idea fairy and say no to requirements that don't align to achieving core objectives. Finally, though you should attempt to develop a thorough plan that accounts for all stakeholders, you should expect it to change. To borrow from President (the General) Eisenhower, "Plans are worthless, but planning is everything."

Thought Leadership for the Federal Enterprise Risk Management Community

Considerations and Best Practices

- Honest assessment of your organizational and process maturity to handle GRC technology
- Develop a clear roadmap with end state clearly defined
- Ensure all stakeholder expectations are identified and accounted for
- Ensure the required resources and funding are available and supported by leadership
- Clearly define key business requirements and prioritize them upfront
- Conduct a thorough evaluation of technology and make selection based on rationalized business requirements and priorities
- Identify sources of legacy ERM data and assess data quality health
- Develop data migration strategy

Common Pitfalls and Lessons Learned

- End goals not clear
- Narrow vision and scope with point solutions addressing current pain points only
- Technology defining business requirements rather than the other way around
- Lack of committed resources due to competing priorities
- Technology selection without careful evaluation of key business requirements
- Hidden costs of implementation
- Project governance not established
- Legacy data is scattered, disorganized, and is not of good quality

During Implementation

When a GRC implementation project is underway, program leaders should try to maintain everyone's focus on keeping their eyes on the road. Problems will arise and environmental changes are bound to happen but an unwavering resolution to move forward with delivery is what sets successful leaders and projects apart. The mantra to indoctrinate GRC project leaders is to 'Be Agile but stay focused on the finish line.' Do not let perfection be the enemy of good (or good enough) as there will always be a trouble log.

Considerations and Best Practices

Plan for ongoing Stakeholder engagement and communications, expectation management during implementation

- Prepare to deal with cultural resistance and leadership changes and have contingency plans
- Ensure adequate program management is in place
- Implement and adhere to a well-defined process for dealing with (technical) change and technology challenges during implementation
- Plan for and closely monitor data mapping, transformation, quality, and governance. Perform data cleanup as appropriate, prior to migration

Thought Leadership for the Federal Enterprise Risk Management Community

- Execute on plans for archival and storage of legacy ERM data that does not require to be migrated to the GRC platform
- Ensure that the infrastructure required to support technology integration remains intact and current

Common Pitfalls and Lessons Learned

- Key stakeholders not engaged in requirements identification and design vetting
- Too much complexity and scope (trying to solve everything)
- Stakeholders trying to bring a lot of unnecessary legacy data onto the GRC platform
- Infrequent or inadequate project communications
- Lack of attention to Change Management and how it affects your people

The project doesn't end once the technology is live. Quite the opposite actually, as most of the long work is just beginning. Even when implemented, technology solutions (and users!), require continued attention. Now it's time to focus on arguably the most difficult part: customer satisfaction and engagement. Stakeholder engagement remains a constant and top priority, and nothing should be dismissed or you risk failed adoption. Put simply, if it's broken, fix it! Be prepared to market your work as well and use the tool to tell the success story. Lastly, be sure to stay on top of tech debt and be future proof but know when to move on.

Considerations and Best Practices

- Develop and resource a plan for user training and support
- Provide adequate means for reporting and usability enhancements
- Build a two-way street for feedback and continuous improvement
- Continue to monitor integration with other non GRC systems and support from infrastructure
- Continue planning for the next phase and any application version upgrades or additional enhancements
- Ensure sufficient resources remain available for ongoing Technical Support
- Finally, be sure to apply the previously developed Metrics to assess your ROI

Common Pitfalls and Lessons Learned

- Assuming that delivery = success
- Poor adoption: lack of buy-in, waning leadership support, training, personnel turnover
- Lack of future budget for training, maintenance, and support
- Failure to stay aware of evolving technology, new solutions and integrations
- Not keeping up with version upgrades, facing end-of-life issues

The Future of GRC Technology Looks Promising

The market continues to mature in terms of the extent and depth of solutions available, and there are many different solution offerings now available to address newer risk management challenges such as Environmental Social and Governance (ESG), Diversity Equity and Inclusion (DEI), and financial crimes,

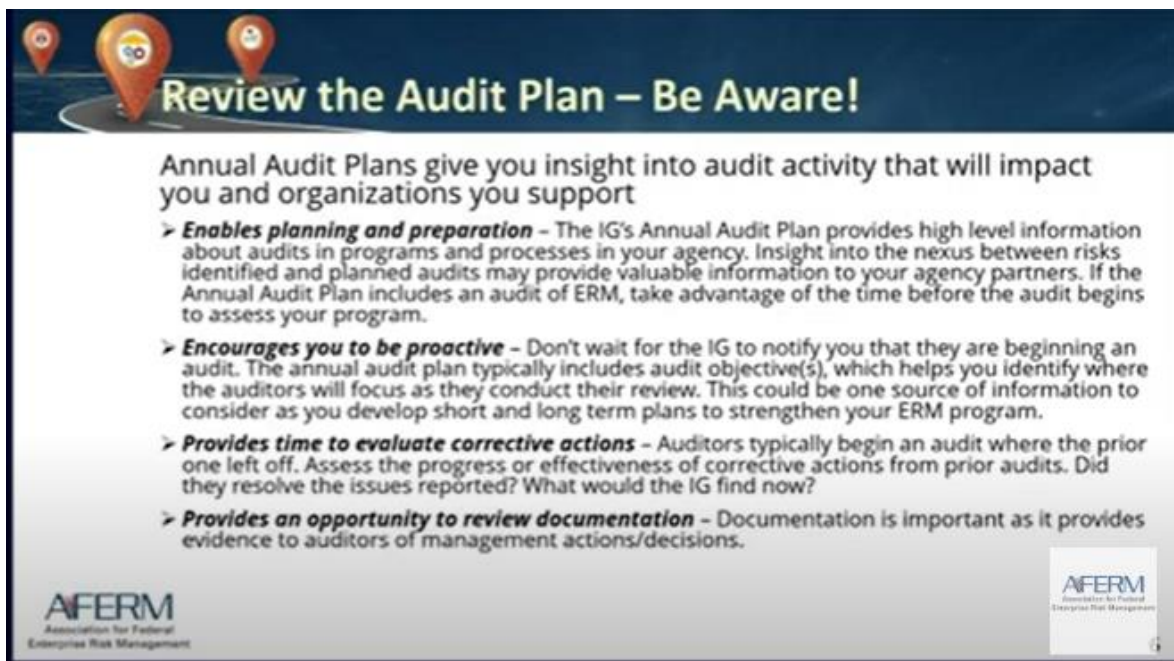
Thought Leadership for the Federal Enterprise Risk Management Community

beyond the traditional domains of financial, operational, and cyber risk and compliance. At the same time, organizations must also improve and mature their use of the technology to help fully realize the potential benefits offered through automation, and drive integration of risk management functions across the enterprise. The integration of traditional GRC tools with advanced data modeling and artificial intelligence (AI) capabilities has opened new vistas in exploring further maturation of ERM functions. However, before launching into the exploration of these new and wonderful capabilities, a multi-year vision and strategy must be established along with a target operating model. Implemented and managed with a well architected strategy and plan, ERM/GRC solutions can become powerful tools for the company for risk aggregation and integrated reporting, risk analytics, and decision support.

Audit Tips & Tricks

[Are you Audit Ready?](#)

Check out this Session from AFERM 2022 Summit



Review the Audit Plan – Be Aware!

Annual Audit Plans give you insight into audit activity that will impact you and organizations you support

- **Enables planning and preparation** – The IG’s Annual Audit Plan provides high level information about audits in programs and processes in your agency. Insight into the nexus between risks identified and planned audits may provide valuable information to your agency partners. If the Annual Audit Plan includes an audit of ERM, take advantage of the time before the audit begins to assess your program.
- **Encourages you to be proactive** – Don’t wait for the IG to notify you that they are beginning an audit. The annual audit plan typically includes audit objective(s), which helps you identify where the auditors will focus as they conduct their review. This could be one source of information to consider as you develop short and long term plans to strengthen your ERM program.
- **Provides time to evaluate corrective actions** – Auditors typically begin an audit where the prior one left off. Assess the progress or effectiveness of corrective actions from prior audits. Did they resolve the issues reported? What would the IG find now?
- **Provides an opportunity to review documentation** – Documentation is important as it provides evidence to auditors of management actions/decisions.

AFERM
Association for Federal
Enterprise Risk Management

AFERM
Association for Federal
Enterprise Risk Management

Thought Leadership for the Federal Enterprise Risk Management Community

Corporate Sponsors

Thank you for your support!

Platinum Sponsors

Deloitte.



**KEARNEY &
COMPANY**



proofpoint.

workiva

Silver Sponsors



RSA

