EXECUTIVE REPORT 2016

AGA®

2016 ERM and Internal Controls Forum
Summary | Washington, D.C.

ACKNOWLEDGMENTS

Technical Committee

Government

Mark Reger, Deputy Controller, OMB

Regina Kearney, Policy Analyst, OMB

Cynthia Vitters, Senior Advisor, OMB

AGA Corporate Partners

Dan Murrin, Forum Co-Chair and Partner, EY

David Zavada, Forum Co-Chair and Partner, Kearney & Co

Wendy Morris, Director, MorganFranklin Consulting

Sallyanne Harper, Vice President/Exec. Officer, AOC Solutions

Howard Campbell, Director, IBC a DBS Company

Ted Kozlow, Principal Consultant, IBC a DBS Company

Damon Sutton, Principal, Castro & Co

Eric Rasmussen, Partner, KPMG

Laurie Patton, Sr. Manager, EY

Daniella Datskovska, Sr. Manager, EY

AGA is proud to recognize our sponsors for their support of this effort. (See page 23)

Executive Report Contributors

AGA

Ann M. Ebberts, Chief Executive Officer

Susan Fritzlen, Chief Operating Officer

Elizabeth H. Barnette, Marketing & Communications Manager

Anna Schumann, Communications & Marketing Manager

EY

Dan Murrin, Partner

Daniella Datskovska, Sr. Manager

Adam Peters, Manager

Marc Pratta, Manager

Kearney & Company

David Zavada, Partner

Alyssa Fusisi, Sr. Manager

Erin Dunkum, Sr. Manager

Jenna Blouch, Sr. Manager

Sean Vineyard, Sr. Manager

Chantz Beck, Sr. Manager

Wes Hogan, Sr. Manager

Geoff Hoehn, Manager

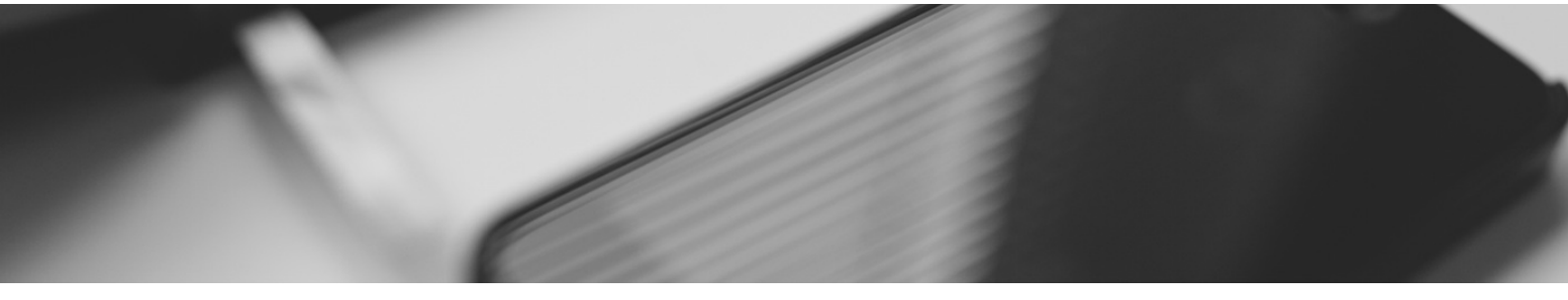
Liz Pierpoint, Manager

AGA's ERM and Internal Controls Forum was developed out of AGA's Corporate Partner Advisory Group's (CPAG) Accounting and Auditing Committee for the purpose of bringing federal government and private-sector executives together to discuss the upcoming policy update to the Office of Management and Budget's (OMB) Circular A-123, which will provide guidance on enterprise risk management (ERM) at the federal agency level.

The mission of the CPAG is to bring industry and government executives together to exchange information; support professional development; improve communications and understanding; solve issues; and build partnership and trust, thereby enhancing AGA's focus on advancing government accountability. This is accomplished by providing studies and analyses of public-sector financial management; providing input to AGA for the purposes of informing government on the possible impacts of industry trends and best practices in financial management; and facilitating a neutral platform for dialogue and collaboration between government and industry.

CPAG is a network of public accounting firms, major system integrators, IT companies, management consulting firms, financial services organizations and education and training companies that all have long-term commitments to supporting the financial management community and choose to partner with and help AGA in its mission.

TABLE OF CONTENTS



EXECUTIVE SUMMARY

On April 25, 2016, the AGA ERM and Internal Controls Forum (forum) brought together leaders from the federal government and private sector risk management and internal control communities. The objective of the forum was to discuss the upcoming policy update to Office of Management and Budget's (OMB's) Circular A-123, which will provide guidance on enterprise risk management (ERM) at the federal agency level.

Dave Mader, OMB Controller, shared his perspectives at the opening of the forum. He acknowledged the significant number of initiatives that the federal government community is addressing, specifically, the move to shared services and the adoption of the Federal Information Technology Acquisition Reform Act (FITARA) and the Data Accountability and Transparency Act of 2014 (DATA Act), and now a focus on ERM. "In the fourth quarter of this administration is exactly when to think of risk, risk in the context of a new administration. We can provide an honest-to-goodness data-driven assessment of the risks agencies are facing. I think ERM will go down as a hallmark of this transition," Mader said.

Forum panelists included representatives from federal agencies and AGA's Corporate Partner Advisory Group (CPAG).

Forum attendees included federal agency representatives involved in their agency's OMB Circular A-123 initiatives, OMB personnel, the inspector general (IG) community and private-sector employees providing support to federal agencies for these efforts.

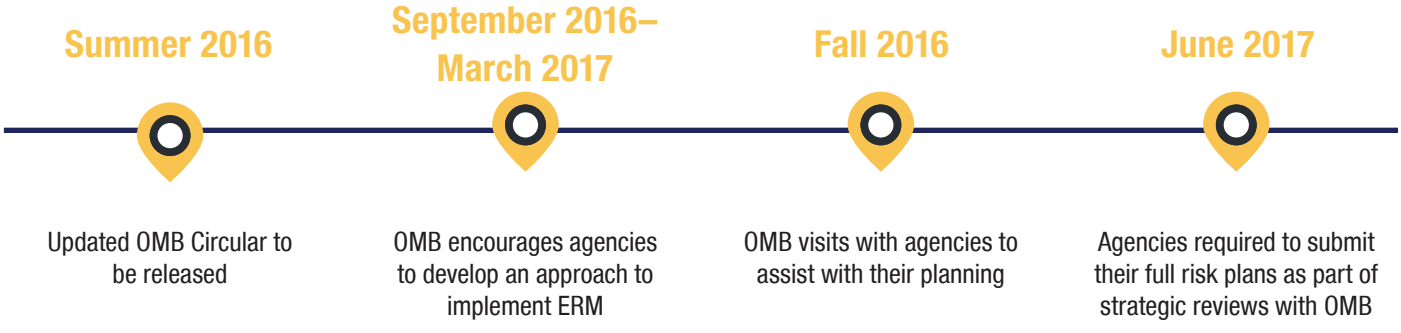
OMB and the federal chief financial officer (CFO) community have spent the past 25 years strengthening internal controls and now is the time to utilize this knowledge to better execute agency and program missions. OMB encouraged forum attendees to consider how internal controls can be applied to the broader federal audience outside of the CFO community by sharing what the CFO community has learned across numerous programs from a broad set of agencies through the former Circular A-123.

Three themes emerged from the forum: (1) ERM standards are directional and not meant to be prescriptive, leaving flexibility at the agency level to determine how best to meet the standards; (2) the importance of a proper governance structure with representative senior leadership across the enterprise, including performance, risk, data analytics and other mission critical areas to require enterprise-wide identification of risks, and provide leadership the ability to make integrated and informed risk-based decisions; and (3) implementing ERM is a long-term process requiring gradual organizational and cultural changes to develop and embrace risk management as a beneficial management approach.

In terms of when the ERM-specific policy guidance will go into effect, OMB presented the timeline illustrated in **Figure 1**.

The following sections provide a detailed summary of the forum presentations and responses to discussion questions.

Figure 1: OMB Timeline



SETTING THE STAGE

Panel Moderator: **Dan Murrin,** Forum Co-Chair and Partner, EY

Panelists: **Mark Reger,** Deputy Controller, OMB; **Dustin Brown,** Deputy Assistant for Management, OMB; **Lesley Field,** Deputy Administrator for Federal Procurement Policy, OMB; and **Karen Hardy,** Deputy Director (Dir.) for Risk Management, Department of Commerce (Commerce)

Concept 1: Prepare for the updated OMB Circular A-123

The updated Circular A-123 will ask agencies to complete a risk profile, develop a risk response plan, explain actions taken to mitigate risks, and participate in an annual discussion with OMB to review approaches and findings, according to OMB representatives.

OMB is focused on the following activities in tandem as they prepare to release the updated policy guidance to incorporate ERM:

- Identify best practices in the commercial sector (e.g., private, public and international) and bring best practices from high-performing organizations into the federal government.
- Develop more rigorous definitions for goals and objectives at different levels of the organization, and incorporate a strong performance management process at each level of the organization.

> **"It is important everyone is engaged in working together to operationalize the agency's mission and activities."**
>
> —Dan Murrin, Forum Co-Chair and Partner, EY

- Assist agencies in developing the proper mechanisms to ensure risks are brought forth to management and the proper information is available to develop actionable plans.
- Work closely with agencies to standardize objectives and make an assessment of federal agencies' progress over time.
- Tailor guidance to have a government-wide requirement, but still provide flexibility in guidance implementation due to agencies' unique cultures, routines and practices as well as their size and mission complexity.

OMB also made the point that ERM is a "career initiative" — it is a long-term process and should be incorporated within all communities and programs, not just the financial community. We need to collectively work to develop strategic and performance plan goals and objectives and make sure it all aligns with ERM.

Concept 2: Mitigate procurement process risks

The federal acquisition community has a structured process to mitigate and share risks with the contracting community. Prior to 2008, there were inconsistencies in the acquisition process because of its complexity. As a result, drawing from the GAO framework, a standard guidance approach was integrated into Circular A-123 activities highlighting:

1. Organizational alignment and leadership, which elevated the chief acquisition officer in all agencies;
2. Policies and processes, which looked at ways to share risks;
3. Human capital policies including requirements for contract officers, contracting officers' technical representatives and program managers, and training development standards; and
4. Information management and stewardship, which developed acquisition labs to focus on innovation and improve the acquisition process.

OMB is collaborating with agencies on using ERM to refocus efforts and ensure they are looking across the GAO acquisition framework dimensions, working with other communities, and breaking down silos.

> **"We have FPDS, which needs to be improved through innovation. I'd encourage each agency to create an innovation lab."**
>
> —Lesley Field, Deputy Admin., Office of Federal Procurement Policy, OMB

Concept 3: Evaluate how risk affects the entire organization

ERM really emerged 10 years ago when *ISO 31000, Risk Management — Principles and Guidelines* was issued, providing a universal language for risk management. This brought together countries and sectors to ask, "How do we practice risk management?" ERM requires thinking and acting with the mindset of how risk can affect the entire organization. Karen Hardy discussed ERM in terms of its impact on the entire organization regardless of where risk manifests itself. She gave an example of a major chain store data breach in 2013. Even though it was an IT breach, it affected the entire organization, including performance, and ability to meet overall organizational and business goals. It cost the company millions of dollars and affected its own and its vendors' reputation.

"You can manage your risk in Information Technology but it also affects other areas (e.g., performance, financial and reputational). The driver of ERM is not to look at risk from a silo point of view but how a risk affects the whole organization."

—Karen Hardy, Deputy Dir. for Risk Management, Commerce

DRIVING CHANGE: THE PATH TO ERM

Panel Moderator: **David Zavada,** Forum Co-Chair and Partner, Kearney & Co

Panelists: **Sheila Conley,** Deputy Chief Financial Officer (DCFO), Department of Health and Human Services (HHS); **Cynthia Vitters,** Senior Advisor for ERM, OMB; and **Mike Wetklow,** DCFO, The National Science Foundation (NSF)

This session provided a discussion on practical ERM implementation best practices from the experience of HHS, OMB and NSF. To guide the panel discussion, five questions were posed. The following provides a summary of their responses and discussion:

Question 1: Can you explain the relationship between ERM and internal controls?

First it was noted that ERM and internal controls are very different. The underlying objective of the Federal Managers' Financial Integrity Act (FMFIA) requires agencies to have internal controls in place to ensure the proper reporting of financial activities, compliance with the wide array of laws and regulations, and efficient and effective operations. Over the past 35 years under OMB Circular A-123, internal control has become the purview of accountants. Circular A-123 has been the OMB flagship circular, and each iteration of A-123 has challenged agencies to take their efforts to the next level. Ten years ago, Circular A-123 revisions changed the internal control focus towards financial reporting, but for today's environment this perspective has broadened. While internal controls are used to manage risk and meet objectives, for other risks, no controls exist — they are simply policy or other business decisions. ERM provides the opportunity for the federal government to go beyond internal controls by embracing the following actions:

1. Promote a risk-aware organizational structure throughout the organization, beyond just the accounting community. A key element for promoting a risk-aware organization is to develop a normalized language and taxonomy that goes across disciplines and is understood at each level of the organization. Another critical factor is to engage the entire CxO community in this process to ensure collaboration among leaders from across the enterprise to drive this important initiative.
2. Develop a comprehensive view of risk in terms of the agency's mission and objectives. Agencies were not created to just do accounting, but to execute missions and important programs for the benefit of the American public. Having a portfolio view of risk is a disciplined approach to looking collectively at risks to address those that could actually prevent an agency's mission from being achieved.

3. Develop a risk appetite that not only addresses quantitative calculations of materiality risk, but also considers qualitative factors. Only by considering both factors are agencies able to have open and candid conversations about the risks they are willing to accept.

"The risks that really matter deal with the 75 percent of the budget allocated to the agency's mission."

—Deb Jeffrey, IG, CNCS

The panel emphasized that implementing an ERM practice is a journey and not a compliance exercise. Implementation will not occur overnight and there may be times where agencies may need to revisit the beginning stages of implementation due to changes in leadership or other factors.

Question 2: Who should lead ERM?

True success comes with the integration of cultural and organizational change. The panel expressed the importance of ensuring those responsible for leading ERM:

- Have the ability, focus and pull within the organization to actually drive ERM implementation and influence the culture around risk tolerance;
- Realize ERM extends beyond the financial community to include the performance improvement and data analytics communities; and
- Customize ERM governance to the organization and existing culture.

It was also advised to implement a principled approach that supports a culture of bringing people to the table to discuss organizational risks, but noted that it can take time for senior leadership to get comfortable discussing risk topics.

"True success is measured by a cultural shift in reporting risk and a program customized to fit the agency."

—Cynthia Vitters, Sr. Advisor, ERM, OMB

Where the ERM function resides within the organization depends significantly on the culture of the organization and the command, respect, and ability of the individual in charge to reach senior management. There are many strong opinions that the CFO not lead ERM, but this is not necessarily true for all organizations, as the CFO community has experience with risk management and subsequently, a lot to offer when it comes to ERM.

Question 3: What are the biggest challenges to implementing ERM?

According to panelists:

- ERM is a not a quick "check the box" exercise. Implementing ERM requires a total culture change, which takes time to integrate throughout the organization. It is important to receive buy-in from senior leadership across the organization, which in turn builds trust and confidence in the ERM process.
- Finding individuals willing to step into the CRO role due to perception that if things go south, the CRO will be held responsible. In reality, the CRO's main objective is to facilitate leadership in the identification and management of risks. The CRO is the organization's "risk facilitator," not the "risk owner."
- Finding and retaining the right mix of talent as there is currently no job series in the federal government for the skill set needed, and the skill sets that have been successful so far have varied.
- Ensuring leadership understands and takes ownership of risks. Leaders need to feel comfortable that they will not be reprimanded for identifying and communicating risks.
- To build bridges between organizational silos, discussion needs to shift from the "what" associated with technical requirements, to "how" different organizations manage their risks. More often than not, this shift in discussion identifies existing risk management processes and procedures, and it is a matter of connecting the dots to achieve integration at a more strategic enterprise level.
- For organizations who currently have risk management processes under Circular A-123, aligning these processes to minimize overlap or redundancy when developing risk profiles and aligning identified risks to existing control activities.

The results of the audience poll to this question supported many of the challenges identified by the panelists, including:

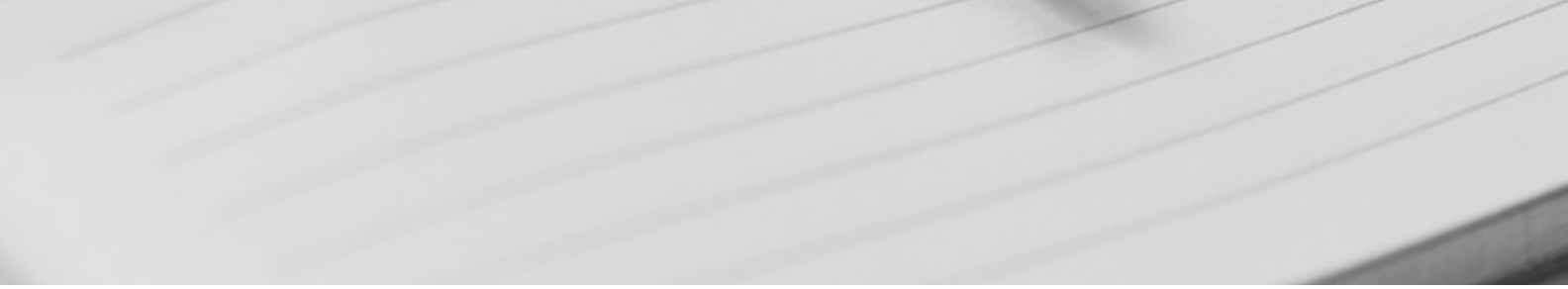
41% the ability to have open and honest discussions of risks

25% challenges associated with breaking organizational silos

12% employing training and achieving technical understanding

11% resource constraints

10% integrating/aligning related activities



The panelists also coupled this discussion with identifying opportunities and noted that opportunities exist to identify trade-offs associated with establishing a risk appetite, specifically the amount and type of risk an organization is willing to take to meet their strategic objectives. This provides more latitude for federal agencies operating under limited resources, and for taxpayers not willing to pay more in tax revenue to meet a limited risk appetite. There is both opportunity and challenge working with the GAO and IG communities to develop the language to communicate the trade-offs associated with risk appetite. Organizations need to be prepared to communicate these trade-offs to Congress and the public if an unfavorable event occurs.

Question 4: What are the keys to making ERM an integrated process?

The panelists stressed that an ERM approach should start small and grow strategically over time. Key starting points include:

- Developing an inventory of existing risk management processes occurring across the agency;
- Identifying threats and opportunities within current risk management processes;
- Assigning and prioritizing risks to first identify the risks and then holding candid conversations with individuals who have knowledge of the agency's programs and how they operate;
- Establishing a governance body to oversee ERM, as it plays a critical role in ensuring success. A best practice is for the key individual responsible for the ERM program (usually the CRO) to report directly to the organization's COO (or deputy secretary or undersecretary for management); and
- In identifying individual leaders for programs, it is important to consider their prominence within their organization and access to key leadership rather than just background and technical skill set.

Question 5: What next steps can agencies take in implementing ERM?

The panel agreed that next steps for implementing ERM largely depends on where an agency is now. Panelists stressed the importance of starting with a realistic implementation plan that involves a phased approach. An implementation plan aids in communicating the agency strategy and measuring progress.

Panelists also emphasized the importance of communication throughout the process, including developing and maintaining a common language that everyone uses. Equally important is establishing a process of governance in which communication flows through the agency. There is no "one size fits all" approach and the form and structure will differ depending upon the agency mission, culture and goals.

Finally, it is important to develop the agency's initial risk profile. The risk profile serves as a building block from which to start risk conversations. A key success factor is to educate everyone involved, and keep in mind that there are resources in the community to reach out to for help.

AUDIT PANEL

Panel Moderator: **Eric Rasmussen,** Partner, KPMG LLP

Panelists: **Brett Baker,** Asst. Inspector General (IG) for Audit, NSF; **Alvin Brown,** Deputy Asst. IG, United States Agency for International Development (USAID); **Deb Jeffrey,** IG, Corporation for National and Community Service (CNCS); **Kristen Kociolek,** Asst. Dir., Government Accountability Office (GAO); and **Lori Pilcher,** Regional IG for Audit, HHS

The panel was composed of agency representatives from the IG community discussing pending updates to Circular A-123, the relationship between auditors and agencies in the context of the concept of auditor independence, and transparency between auditors and agencies.

Concept 1: The relationship of the auditor/IG community with the agency

The IG community panel began by suggesting that agencies meet regularly with the IG community to collaborate on identified risks. Due to limited resources, work performed by auditors is usually risk-based, and risk is constantly assessed to determine where work should be performed. Auditors should be mindful of the potential risk of compromising independence when collaborating with an agency, and close collaboration can pose challenges with independence. To best mitigate this risk, auditors should allow agencies to own their risks and processes, and make decisions as to how they will be managed providing appropriate technical insight and knowledge while maintaining independence.

Concept 2: Promoting transparency with the IG and agency relationship

Auditors can no longer take the traditional approach, waiting to see what activities happen when, then going back to see what was wrong with those activities. Information needs to be shared on a real-time basis and auditors should share with agencies the actions that will occur using the information gathered as well as if that information will serve as a basis for an investigation. Auditors are experienced with ERM and their knowledge should be used to assist agencies with managing risk as typically, auditors do not have a policy-based agenda that would lead to the minimization, misrepresentation or understatement of risks. Auditors can assist with the identification and assessment of risk subsequently assisting agencies in their ability to prioritize risks and decide how to dedicate resources to mitigate those risks.

Concept 3: How auditors and agencies should work together identifying root causes

The IG community panelists said auditors should have visibility into the corrective action process as it matures, providing more confidence in the thoroughness and rigor of the process, and reducing their likelihood to question the results. An auditor's goal is to enlighten agencies about risks and prepare for necessary corrective actions; however, panelists agreed agencies should not rely on auditors to identify root causes for deficiencies. It is the agency's responsibility and in their best interest to perform assessments, which helps maintain auditors' independence.

Concept 4: Criteria for assessing an agency's risk appetite and risk profile

The IG community panel stressed the importance of auditors first assessing where agencies are in their ERM process by asking certain questions, such as:

- What are the standards for developing ERM processes?
- How are risks being communicated across the agency?
- Are procedures being applied consistently?
- How are risks being defined and are they understandable?
- Is there training available?
- How are data points established?
- Are reporting systems reliable and providing meaningful information?
- How is information translated from the agency's risk registers to the agency's risk profiles?
- What 'buckets' or categories of risk is the agency assessing and how did they determine them?
- What are the elements that would cause you (or your program) not to succeed?
- What is the agency using as supporting documentation for decisions?

Concept 5: Factors agencies should consider when establishing and tailoring a fraud risk framework

The IG community panel insisted auditors and agencies review the GAO Green Book Principle 8 — Assessing Fraud Risk. This principle is meant to assist agencies in establishing processes to address and assess fraud risk, as it is one of the many factors to consider when developing an agency's risk appetite. Risk appetite will vary from agency to agency because certain risks are more significant at some agencies than others. As a result, agencies need to consider fraud risk in the context of all of their identified risks. GAO has also developed A Framework for Managing Fraud Risks in Federal Programs to assist agencies in discerning the unique risks associated with fraud. Fraud risk frameworks have improved in recent years through the translation of information into transaction-level financial detail. This information can be harnessed by establishing automatic triggers within systems or tools to monitor for key fraud risk indicators.

"IGs have a lot to bring to the table. We have no agenda to misstate risk… IGs are not enemies of risk. We want agencies to take on risks knowingly. And, if we aren't invited to the party, the only way to involve us is as a critic."

—Deb Jeffrey, IG, CNCS

INDUSTRY PANEL

Panel Moderator: **Ann Ebberts,** Chief Executive Officer, AGA

Panelists: Edmund Green, Managing Dir., KPMG; **Bailey Jordan,** Partner, Grant Thornton LLP; **Michael Herrinton,** Partner, EY; **Todd Grams,** Dir., Deloitte; and **David Zavada,** Partner, Kearney & Co

The industry panelists represent a knowledge base gained from working across multiple organizations, both public and private sector, in turn providing a more complete knowledge of what works and what does not work, the environmental variables associated with success and leading practices. Following the introduction, each panelist took turns sharing their experiences.

Concept 1: Fundamental ERM building blocks

Green identified certain fundamental building blocks that he feels are necessary in order for an organization to be successful implementing ERM. These building blocks include a strong governance process, performing a risk assessment, reporting on risks, and developing and facilitating training.

To establish a strong governance process, senior management needs to establish the model conditions for something like ERM to be successful. The mandate needs to come from the top of the organization and trickle down through the various layers of management. Green also expressed the importance of developing an enterprise risk profile following a risk assessment, which, assists in vision delivery, identifying impact strategies, and in some cases influencing the overall business model.

From a reporting standpoint, Green urged providing meaningful risk insight to senior leadership to help emphasize what might happen. Reporting should be aimed at identifying the top 10, but no more than 15, critical risks to the agencies' mission, strategies, or business model that senior leadership should focus on. Green stated the biggest challenge in the private sector has been the culture change requiring training to reset the default settings of people's behavior. It is important to align rewards and incentives to induce the type of behavior the organization would want employees to engage in when they are not otherwise told what to do.

Concept 2: ERM in the making

Jordan provided an example of one of his private-sector clients, a publicly listed multibillion-dollar retailer, that implemented ERM. The request for ERM came from the organization's audit committee, and the board of directors established an executive leadership team (ELT) as the owner and the CEO as the chair of the ERM initiative. For day-to-day activities, an ERM working group was formed and facilitated by the vice president (VP) of internal audit, and including two senior VPs and five VPs. The ERM working group had three goals for its ERM initiative, which include:

1. Identify, prioritize, manage and monitor key risks.
2. Start slow.
3. Build a structure and discipline.

The process to achieve these three goals involved a few different methods and inputs. Questionnaires were issued to VPs who rated risks on a scale of one to five based on the likelihood of risk occurrence. One-on-one interviews were held, during which 30 VPs provided their input as to what risks the organization faced. Additionally, results of other risk assessment initiatives performed by other parts of the organization were leveraged. As a result, approximately 100 risks were grouped into common themes to end with an overall high-level risk number of 50.

The working group narrowed the 50 high-level risks to just the top 10 to 15, which were vetted through the ELT and CEO and then presented to the board. Jordan pointed out that if they had stopped at this point, all that has really been accomplished is "list management" and not "risk management." The top 10 to 15 risks were assigned to members of the ELT to develop strategies to decrease the risk to a level that met the organization's risk appetite.

Jordan further explained that as the organization evolved and matured, they developed more of a bottom-up risk assessment approach. To save time and prevent performing interviews with thousands of employees, regional VPs were asked to rank 20 identified risks into a list of the critical top 10. Additionally, if the regional VP was aware of a risk not included in the top 20, they were to add it to their list. As a result, two additional risks were identified. For next steps, the organization started to look at risk appetite and risk tolerance and continue with the bottom-up risk assessment approach.

Concept 3: Challenges in implementing ERM

Herrinton explained that the biggest challenge to implementing ERM is making sure it is a dynamic and ongoing process. The structure of ERM governance and establishing the "tone at the top" is also a challenge, but the biggest challenge will be embedding this structure into the daily activities organizations use to manage their business. For example, agencies should be thinking about risk from the standpoint of how it affects the development of their strategic plan, periodic performance reviews and other uncertainties that need to be addressed to achieve risk management. Successful ERM development requires everybody in the organization to have their hand in considering potential risks and uncertainties and putting the right actions in place to mitigate those risks to the acceptable level so the organization can achieve the intended outcome. In Herrinton's opinion, if this is a part an organization's objective, it has a fighting chance to be successful in ERM. If it isn't, ERM can easily become "list management" and it will seldom move beyond the basics of ERM. Herrinton explained that if risk management professionals truly understand the objectives of ERM, they will be successful implementing risk management.

Concept 4: Successfully implementing ERM

Grams discussed assistance he provided to the Department of Veteran Affairs and the Internal Revenue Service developing and implementing an ERM program. Grams said he believes when implementing an ERM program, it is important to understand that it will take several years to have a fully mature program in place and during implementation, since this is a new concept, agencies will face resistance. Given these facts, Grams stressed focusing on three ideas to achieve success when interacting with program offices or business units:

- Build upon what business units already have — in the federal space, risk management is already a part of the daily activities of federal employees. Recognize this and give them credit for what they are already doing.
- Recognize the culture of the business units and try to understand personalities to know who will support or oppose ERM implementation.
- It is best to start small, finding individuals who will help move the program along faster and become disciples of ERM. These individuals will help spread the program across the agency.

Grams explained that the benefits of ERM are what he refers to as "Up, Down and Across" as follows:

- **Up**: Brings to leadership's attention potential negative issues that could affect the organization. As a result, when defining and determining how to mitigate risks, chances are it may increase the likelihood of receiving resources needed to manage those risks.
- **Down**: People are afraid to share risks. In the recent Federal Employee Viewpoint Survey (FEVS), survey question 17 asks, "Does a Federal employee feel they can raise a violation of law, regulation or policy to their supervisor without fear of retribution?" Survey results disclosed 40 percent of federal employees answered "no." Participating in and embracing ERM can lead to culture change and make employees feel more comfortable in communicating risks to leadership without fear of retribution.
- **Across**: Involves working with counterparts throughout the agency to explain that ERM is meant to help the organization meet its mission goals and objectives. ERM is not a "gotcha" exercise, but a way to drive performance and provide value.

"Make sure not every conversation about risk is negative."

—Todd Grams, Director, Deloitte

Concept 5: Blending and integrating risks into internal controls

Zavada explained that in terms of implementing ERM, it will take a step-by-step approach. Culture change takes time and is truly an evolutionary process. However, agencies can make progress toward ERM by focusing on the short term. In a survey provided to those who have implemented ERM, more than one-third stated that they achieved operational efficiency in terms of risk management, internal control and compliance structure. This improves the information available when making decisions. Zavada believes a short-term focus would leverage the benefits, disciplines and skill sets agencies implemented in their OMB A-123 Appendix A programs. These are skill sets can be taken and applied more broadly in an organization's ERM program. Similarly, the revised GAO internal control standards, if implemented properly, provide a path to ERM.

Zavada outlined some quick wins for agencies to reap the benefits of implementing ERM:

- Align the agency's governance structure — take an inventory of the different governance structures that currently exist and align those enterprise-wide to serve as the agency's ERM governance structure.
- Assess the GAO standards — identify coverage and gaps. Zavada noted a common gap is the risk assessment process and agencies may need to do additional work in this area.
- Take an inventory of current activities — agencies should identify risk management and internal control activities already occurring throughout the agency. This allows agencies to begin to put together the ERM puzzle and build it into an enterprise-wide process.

The panel concluded with three questions posed by Ebberts to the entire panel.

"...the revised GAO internal control standards, if implemented properly, provide a path to ERM".

—David Zavada, Forum Co-Chair and Partner, Kearney & Co

Question 1: How do we keep the momentum going for ERM while new leadership is being identified at the top?

Green said ERM cannot be seen as the latest shiny new object in federal government. For ERM to have staying power, it must be embedded in the management of the organization and how decisions are made. Additionally, the organization needs to demonstrate a clear and compelling value proposition for the benefits of the ERM program — it is necessary for organizations to get their top career people on board. Politicians will be transitioning with the new administration, making it beneficial to have as much buy-in and support from the career individuals who will remain on board. Another benefit would be identifying "wins" within the next nine months to illustrate the value added by ERM programs.

Question 2: Where do you start training when you are implementing ERM?

Zavada explained that ERM training first involves getting the right people in the room and requires an interdisciplinary approach due to involvement across all organizational functions. Additionally, it's important to develop a common language for all parties to ensure they're on the same page and headed down the same path. Panelists added that training needs to start at the top, so leadership can understand and support the program before it is rolled out to the rest of the organization; a common nomenclature helps avoid any confusion with interpreting the ERM message and guidance through the organization.

Green added that his approach looks at training across three levels: a broad-based informative training to all levels that focuses on ERM concepts and values; a high-level training targeted toward the board and senior leadership; and a mid-level management training which focuses more on the detailed execution of an ERM program.

Question 3: How do you work with the culture change while moving forward with implementing ERM?

The panelists were in agreement that having the right leadership will foster the change as well as aligning rewards and incentives to direct federal employee behavior.

BREAKOUT SESSION: SETTING UP EFFECTIVE GOVERNANCE

Panel Moderator: **Daniella Datskovska,** Senior Manager, EY

Panelists: **Debra Elkins,** Dir. of ERM, HHS; **Karen Hardy,** Deputy Dir. for Risk Management, Commerce; **Peggy Sherry,** DCFO, National Credit Union Administration (NCUA); **Doug Webster,** Dir., Government to Government Risk Management, USAID; and **Nancy Potok,** Deputy Dir., Census Bureau

This session provided an opportunity for those who have implemented ERM to share with the government community tips for how to set up an effective governance structure.

Question 1: Why governance in terms of ERM and why now?

- Organization leadership must be involved in establishing a governance structure that effectively manages the implementation of ERM.
- ERM governance plays a key role in the flow of risk information, identifying risk gaps, and in how information is utilized and presented to agency leadership.
- An effective governance structure provides the facilitation needed to integrate the communication across the organization's functional silos by providing the ability to balance risks and objectives with other groups.
- Governance drives who gets what information to manage risk. Governance is needed to balance risks — taking good information that is being managed in silos and bringing it up to a higher level to provide visibility into the enterprise.

Question 2: In your experience, where is the right placement of ERM? Does the size of the agency matter and what drives success in placement?

- Agencies should determine what they want to achieve; what is best for their unique environment, agency culture and challenges; and where ERM champions are located as each agency's ERM implementation will be unique.
- Regardless of where ERM is located, the program needs sufficient support from agency leadership to be successful.
- Placement of the ERM program within the CFO office may cause ERM to be perceived as a compliance-type exercise and one that is only financially focused.

Question 3: What should the chief risk officer (CRO) function be?

- Agencies should identify a central point of contact responsible for the facilitation and coordination of the ERM process across several functional units. The person may be identified as a CRO or equivalent role.
- The CRO or equivalent role should be a senior leadership position that does not require a large support staff.
- The CRO or equivalent role is responsible for facilitating and ensuring agency personnel understand their role in ERM, risk information is inventoried, ERM training exists and leadership has risk information to make appropriate decisions.
- The CRO does not own the risks. The CRO should be a facilitator, manager and communicator.

Question 4: In your organization, what ERM framework was chosen and why?

- Each panelist used a different ERM framework or a hybrid of frameworks — choosing an ISO or COSO framework helps agencies to understand exactly what they are doing and, in turn, guides the implementation of ERM.
- Some mentioned that ISO is shorter and internationally recognized, and some say more understandable, but framework preference all depends on your requirements.
- The selected ERM framework needs to be well understood by the agency and individuals running agency programs.
- The ERM terminology used should be understood by all parties involved.

The main themes of the session were cooperation and collaboration. The panelists understood that the IG community is being asked to take a more active role in assisting agencies along the ERM path. They also understood the stigma that the OIGs at most agencies carry with them is a major hurdle to be overcome.

BREAKOUT SESSION: EXERCISING OVERSIGHT

Panel Moderator: Eric Rasmussen, Partner, KPMG LLP

Panelists: Lori Pilcher, Regional IG for Audit, OIG, HHS; **Carrie Hug,** Dir. of Audit Planning and Implementation, OIG, HHS; and **Deb Jeffrey,** IG, CNCS

Concept 1: Success through collaboration

Agencies can benefit from collaboration with their OIG. As an example, at HHS, the IG provided insight on planning and performing risk assessments in a cost efficient way. This resulted in the program office identifying the areas of risks with its grantees. The program office then shared this information with the IG so they could focus their audits on the high-risk areas of these grantees. This collaboration allowed the program office to put in place an effective risk management process and the IG to focus their audits on high-risk areas in a cost effective way.

Concept 2: The risk level wake-up call

At CNCS, the IG worked with management to develop a risk management approach that focused on the enterprise level. Prior to the collaboration, CNCS conducted their risk assessments based on generic factors. However, more than 50 percent of the grantees that were rated as low and medium were terminated for various reasons (i.e., bankruptcy, performance). Through the collaboration, management was able to put in place a more effective risk management process of their grantees.

Concept 3: Asking the real questions

The panelists concluded that ERM will promote the need for communication between the agencies and their IG's and should consider the following three questions:

- How are we going to be effective partners?
- How are we going to move our programs forward?
- How are we going to communicate, be transparent, and be in it together?

BREAKOUT SESSION: PREPARING A RISK PROFILE

Panel Moderator: Denise Lippuner, Partner, Grant Thornton LLP

Panelists: Cynthia Vitters, Senior Advisor, OMB; **Mark Bussow,** Policy Analyst, OMB; and **Ken Phelan,** CRO, Treasury

This session discussed the upcoming circular updates, implementation timelines and practical guidelines for agencies to advance their ERM programs.

Concept 1: Defining risk profile

A risk profile:

- Identifies key risks, types of risks and the possible effects of risk;
- Is a thoughtful analysis of the risks an agency faces toward achieving its strategic objectives that arise from activities and operations;
- Is a high-level view of an agency's most significant risks for achieving goals and objectives;
- Should assist and facilitate a determination on aggregating types of risks;
- Enables managers to determine how best to allocate and deliver resources to achieve mission objectives;
- Differs from a risk register as it is a prioritized inventory of only the most significant risks and should be considered from a portfolio perspective; and
- Should be approved by an agency risk management council or equivalent.

Concept 2: Expected requirement for OMB policy

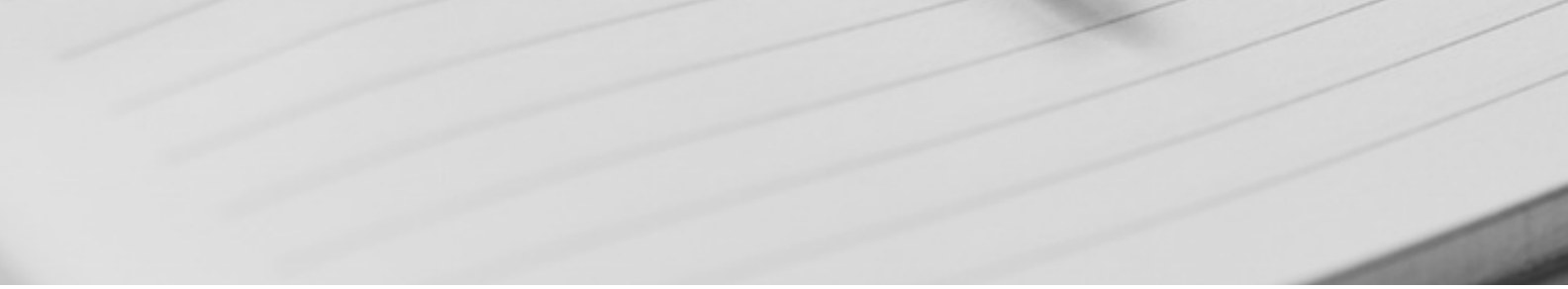
The updated OMB circular will work to integrate content with broader agency governance processes, including the budget process. The following summarizes the discussions related to the expected requirement updates:

- Intended to be an "umbrella" policy that acts at the top level of the organization, but also acknowledges what agencies do through strategic reviews.
- OMB focused on developing effective processes that inform decision-making, which often requires restraint from those in oversight roles.
- OMB cannot provide an array of details and still make the content useful to all organizations; therefore, the circular attempts to integrate with existing processes.
- OMB will provide flexibility to agencies regarding new OMB Circular A-123 requirements and recognizes the process will mature over time.

Currently, the only requirement in the draft circular is the development of a risk profile. The following summarizes discussion related to the risk profile:

- OMB does not intend to mandate that every agency provide a completed risk profile and recognizes the need to provide agencies with the ability to make deliberate decisions.
- Circular will detail the aspects agencies need to address in developing risk profiles.
- Risk profile examples with key elements that should be included will be provided to agencies.
- Flexibility will be provided regarding the actual risk profile construction, form and content to optimize and customize their approach to make it useful for decision-makers.
- Circular will not mandate that agencies establish a risk appetite and risk tolerance. These are considered core principles and part of the governance process, and OMB recognizes the need for flexibility considering varying agency missions.
- OMB is planning an annual discussion with each agency regarding risk profiles and risk assessments for strategic-level decision-making.

In terms of governance, the circular will not have a requirement for a CRO position or the specifics for a structured committee, rather it will recommend a proper governance structure that covers the span of agency functions that should be put in place and will provide examples of effective models.



Concept 3: Implementation timeline

OMB provided an expected timeline (which might shift depending on the specific release date):

- **Summer 2016** — updated OMB Circular to be released
- **September 2016–March 2017** — OMB encourages agencies to develop an approach to implement ERM
- **Fall 2016** — OMB visits with agencies to assist with their planning
- **June 2017** — Agencies required to submit their full risk plans as part of strategic reviews with OMB

Concept 4: Practical considerations for implementing ERM

OMB has organized a working group to develop a playbook on implementing the new OMB circular. The playbook will neither be an OMB document, nor a detailed, prescriptive "check-the-box" or a one-size-fits-all manual. Instead, it will be a joint agency publication that will provide:

- Background to ERM in the federal government;
- Lessons learned from the private and public sectors;
- Basic principles all agencies should follow;
- Basic principles to help to develop an effective ERM culture;
- What is expected, including some repeat requirements of Circular A-123, and how to get started; and
- Appendix of examples (i.e., job descriptions, organizational charts, etc).

Concept 5: Guidance for developing a risk profile

The playbook provides agencies tools needed to develop a risk profile and addresses some circular requirements. Below are steps agencies might use when developing a risk profile (which align to OMB circular requirements):

1. **Identify objectives.** Determine what risks could prevent the organization from achieving its goals and objectives.
2. **Identify risks.** Definition of a risk is "effect of uncertainty on objectives." It is preferable to document risks in a simple and concise manner that communicates the risk's potential impact. ERM is a lot about communication, relationship-building and dialogue. It is recommended that agencies utilize information from the A-123 process, results from EVS scores, OIG audit reports, GAO reports, etc.
3. **Respond to risks.** Document current risk responses (i.e., the action currently being taken to mitigate the risk). It is important not to take accountability away from people responsible for the risks.
4. **Review risks continuously.** Assign a risk owner and conduct an ongoing risk review. Utilize a committee to help prioritize risk and normalize the process. OMB will review agency plans annually.

BREAKOUT SESSION: IMPLEMENTING THE NEW GAO GREEN BOOK

Panel Moderator: Steve Koons, Partner, Cotton and Company
Panelists: Kristen Kociolek, Asst. Dir., GAO; and **Grant Simmons,** Asst. Dir., GAO

This session provided a brief overview of the recently revised *Standards for Internal Control in the Federal Government*, also referred to as the Green Book, issued in September of 2014 and effective in FY 2016. The session took on a question-and-answer format facilitated by the moderator as well as direct questions from the audience. The questions addressed were generally focused on one of the following three key topic areas:

- How the Green Book is organized and recent changes;
- How ERM relates to Green Book principles; or
- Available resources to assist with Green Book implementation.

Concept 1: How the Green Book is organized and recent changes

- The Green Book still includes the five components of internal control (control environment, risk assessment, control activities, information and communication, and monitoring) and the revised version added 17 principles to support the five components. Each principle is codified to provide structure and translates the updated COSO framework to better align to the federal government. The principles help to better articulate and clarify what is required under each component.
- The revised Green Book also includes attributes to further support each of the 17 principles. The attributes, while not required, provide examples of control activities an agency may employ in applying a specific principle and proper documentation to maintain in support of a Green Book assessment.

Concept 2: How ERM relates to Green Book principles

ERM and the risk assessment component of the Green Book are linked as the overall concept of risk management flows through ERM and further down into the level of internal control. While ERM focuses on risk management at more of a strategic level by identifying risks associated with an entity's strategic objectives, at the internal control level, risks are assessed against established strategic objectives. Essentially, ERM sets the strategy for the agency while internal control is the execution of that strategy.

Questions posed to the panelists regarding specific risk concepts included:

- **Fraud risk considerations.** Fraud risk is a topic that was heightened by certain financial crises in recent years, forcing the audit community to employ specific audit standards and steps to assess fraud risk. Consistent with the revised COSO standards, Principle #8, Assess Fraud Risk, was incorporated into the revised Green Book to serve as a reminder to management to be cognizant of fraud risk. The GAO Framework for Managing Fraud Risk serves as a practical application of Principle #8, walking step-by-step through activities that can be employed to manage fraud risk.
- **Reputational risk.** As stewards of public resources, reputational risk will always exist, as the American taxpayers care deeply about how their money is being used. Participating in ERM and internal control implementation through the Green Book standards helps to clarify possible reputational risk for an organization and heightens management's awareness. Ultimately, mitigating reputational risk boils down to the concept of risk appetite and determining if a risk outweighs the associated benefit. While resources may make it impossible to reduce the risk to zero, ERM helps agencies make informed decisions around the risks they are willing to accept.
- **The concepts of risk tolerance and risk appetite.** In the revisions to the new Green Book, GAO spent a considerable amount of time and effort addressing the concept of risk tolerance. Risk appetite is less well-defined because it is established at a strategic level, which resides within an agency's ERM program — unlike risk tolerance, which is developed at the process level. The COSO framework defines risk appetite, and, while the underlying concepts are good, there is some translation necessary to apply it to the federal government, as agencies often operate in high-risk environments (i.e., disaster relief). This proves challenging when applying the COSO's concept of risk appetite to the government. Risk appetite may be further defined within updates to the Circular A-123; however, it will take time for agencies to find the correct approach for defining their risk appetite.
- **Program-level documentation.** The revised Green Book emphasizes that internal controls encompass operational controls in addition to controls over reporting and compliance. The updated Circular A-123 will require that the annual statement of assurance covers internal control over everything, not just financial reporting. When considering the level of documentation needed over a particular program, it is important to keep in mind the significance of the

program to the agency. GAO recognizes that it is difficult to consider each program in the context of the agency's entire operations and that prioritization and communication will be needed to determine the appropriate risk appetite and risk tolerance for each program. Agencies are encouraged to take advantage of the latitude and flexibility provided by the Green Book as long as decisions are justified and documented.

ERM and risk assessment documentation. When considering documentation requirements around an agency's ERM and risk assessment processes, it's important to consider the scale of an agency's operations. For agencies with only a few strategic objectives, documenting the decision process may be fairly simple, involving documenting discussions and meeting minutes around those decisions. For larger and more complex agencies and programs, it may be necessary to develop a database or specific tools to assist in the process. For acceptance of significant risks associated with key strategic objectives, documentation is key to support management's decisions and plans for meeting that objective.

Concept 3: Available resources to assist with Green Book implementation

There is currently no plan for GAO to update the Internal Control Management and Evaluation Tool developed in 2001, but GAO plans to re-visit the idea once the updated OMB Circular A-123 is released. However, the 2001 tool is still relevant and can be used as base for implementation of the revised Green Book with further mapping of the tool to the 17 principles.

GAO is working on two additional products associated with the Green Book and ERM implementation. The first is an evaluation tool for auditors which will focus primarily on the evaluation of the Green Book as part of performance audits. This tool could also be leveraged by agency management to gain an understanding of what auditors are looking for. The second is a report which will discuss leading ERM practices identified from surveying federal entities with more established ERM programs.

While agencies wait on updated OMB guidance and are working on implementation of the revised Green Book, agencies should start taking credit for what they have already been doing and focus on documenting actions supporting sound project management. Agencies can also leverage processes in place that have been successful for assessing internal controls over financial reporting and adapt them to assess controls identified in non-financial reporting areas.

BREAKOUT SESSION: BENEATH THE ERM UMBRELLA — INTEGRATING RELATED EFFORTS

Panel Moderator: **David Zavada,** Partner, Kearney & Co

Panelists: **Mike Wetklow,** DCFO, NSF; and **Doug Glenn,** DCFO, Department of Interior (Interior)

This session discussed best practices and opportunities for organizations to effectively integrate ERM by leveraging existing resources.

Concept 1: ERM is an integrated, interdisciplinary process

ERM should not be a siloed process; it has to be integrated and interdisciplinary. Establishing a foundation for a well-integrated ERM process requires a blend of other management processes to be effective. Agencies should focus on opportunities to align and leverage related risk management and internal control activities. Frequently, "risk management" or "control area" opportunities are not labeled as such, but should be identified and merged into a broader ERM process.

Results were shared from a recent survey conducted by the Association for Federal Enterprise Risk Management (AFERM) and PwC. Since developing an ERM program, 35 percent of agencies have reduced duplicity in risk assessment and/or compliance activities, and 41 percent enhanced decision making by utilizing data and information produced by the ERM program. Wetklow explained that with ERM, if you are successful you might not immediately realize it. As opposed to OMB Circular A-123, when a material weakness is resolved, for example, there is a realized result. ERM is more of a management practice or a culture. This is how NSF is thinking about ERM to help make decisions and cut down existing compliance burdens.

Concept 2: Beneath the ERM umbrella

ERM is a long term process, it's evolutionary, and there are phases to develop a mature process. Illustrated in **Figure 2**, the "ERM Umbrella" graphic represents a maturity model process that is consistent with OMB Circular A-123 and COSO. There are four phases: assessment, planning, coordination and implementation. Within the process, there are focus areas that cut across the phases: 1) leadership and governance, 2) standards, 3) integrating independent risk management activities and 4) integrating independent internal control activities.

Within the cross-cutting areas, there are actions that can be executed now to begin ERM implementation:

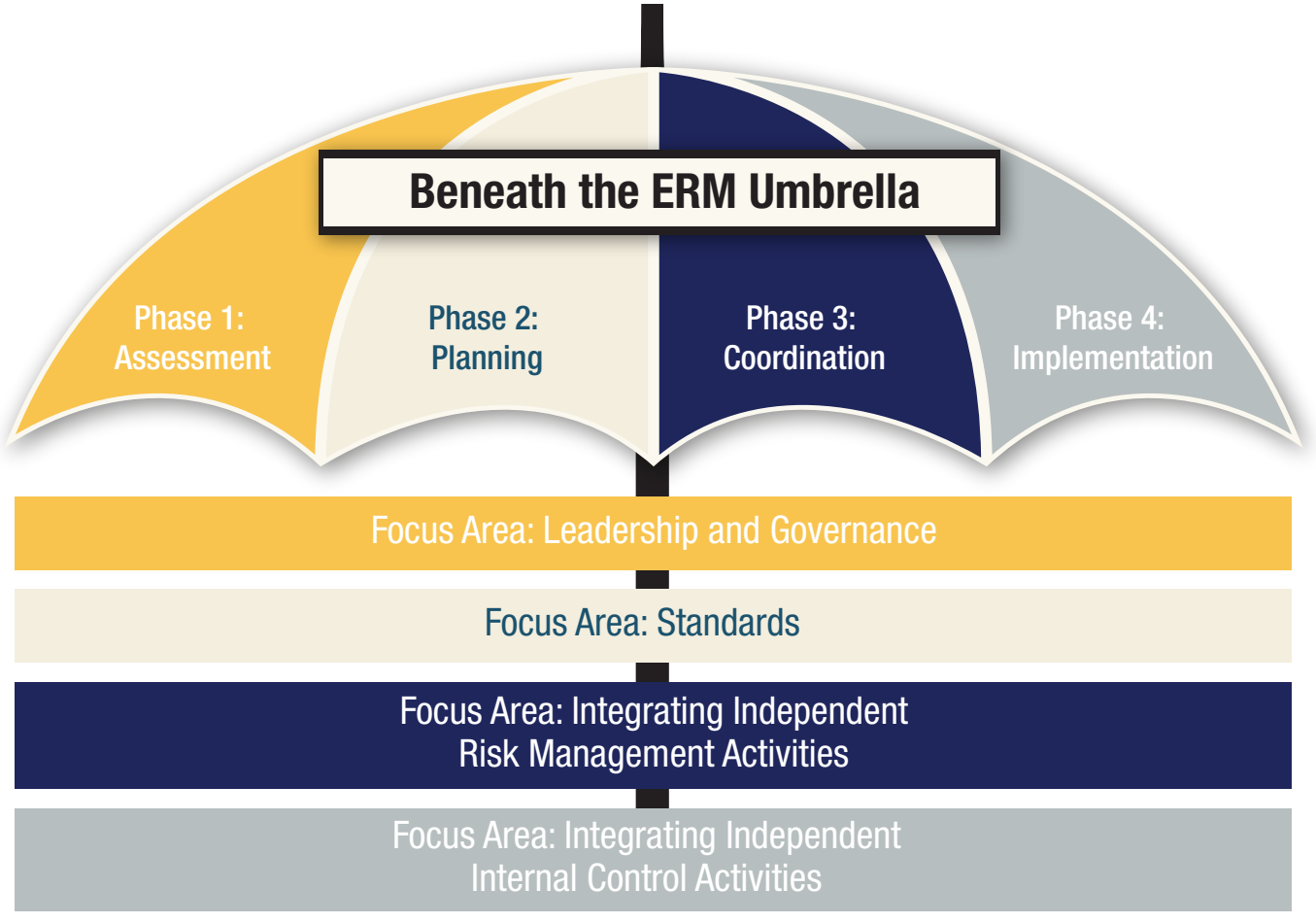
- Define governance. Put in charge an individual who has the organizational clout to get things done. Aligning the governance structure is something that can be done immediately.
- Review GAO and COSO standards to develop a plan. If GAO standards are fully implemented, they cover a significant part of the ERM process and the agency is much farther down the path of ERM.
- Review and leverage other risk management and internal control inventories to assist with ERM efforts and objectives.

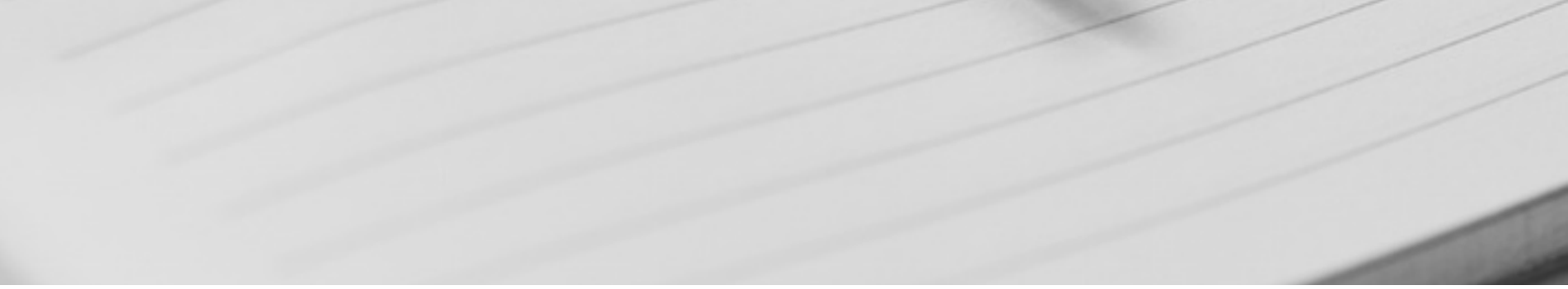
Concept 3: ERM guiding principles

The challenge is to expand beyond financial reporting and emphasize operations that focus on effectiveness and efficiency. CFOs do a good job of managing financial risk, but may struggle outside of finance. The intent of OMB Circular A-123 was never to develop additional work, but to provide agencies tools to implement internal controls more strategically using the ERM framework. The different drafts of OMB Circular A-123 mentioned ERM, but there was minimal guidance and agencies asked for more direction. There are seven guiding principles based on COSO Embracing ERM: Practical Approaches for getting started, that NSF is using to develop the implementation plan that is due in September.

- **Obtain support from the top.** ERM initiatives must be enterprise-wide and viewed by leadership as an important strategic effort. If done correctly, ERM will enhance decision-making and enable agencies to better define and proactively respond to risk. NSF started at the top of the organization and held training sessions with experts to define ERM.
- **Build ERM using incremental steps.** Start small by breaking down ERM into more manageable parts and then grow over time. A great resource is the maturity model, which plots where an entity is within ERM. Also, consider starting with a management function or program office in which risk management processes already occur.

Figure 2: ERM Umbrella





▶ **Focus initially on a small number of top risks.** Identify a small number of strategic risks that are important to agency leadership and that can be managed and then evolve from that starting point. Selecting top interest items rather than a large list will make it manageable.

▶ **Leverage existing resources.** Work with existing staff, management, and working groups with knowledge and capabilities relating to risks and risk management. If done right, ERM can reduce duplicity of compliance efforts. Some performance management offices have apprehensions that it would need additional resources. NSF is setting a goal to use existing resources and do it without additional burden on staff and show it can cut compliance work by building on what is already in place.

▶ **Build on existing risk management activities.** Inventory risk management activities already in place and then align them with the ERM process. Use GAO as a baseline to make cuts and minimize duplication and overlaps. What NSF is learning from this process is how different business processes work and activities to be leveraged in order to cut down on some of the work.

▶ **Embed ERM into the decision-making practices of the organization.** Build ERM as a supporting tool for informing decisions and processes at all agency levels. Build consistent terminology when meeting with leadership or components of the organization.

▶ **Provide ongoing ERM updates and continuing education for leadership and senior management.** ERM is an evolving practice and it's important for leadership to receive updates and best practices.

Concept 4: Broadening the discussion of risk

Glenn discussed the steps Interior is taking to make ERM a broader reality:

- Focusing on a small number of risks such as strategic risks important to leadership.
- Implementing a portfolio view and looking across the department in all disciplines and organizations.
- DOI manages risk in an integrated manner and accepts some level of risk. The OIG, auditors and press are ready to point out the agency's risks, but if we are going to manage risk there has to be some level of acceptance.

"Start with leadership and governance and establish an accountable lead to coordinate ERM implementation."

—David Zavada, Forum Co-Chair and Partner, Kearney & Co

- Risk appetite is the amount of risk that an organization is willing to accept. The risk appetite should be established by senior leadership.
- Risk tolerance is the acceptable lever of variance relative to achievement of objectives.

Quick wins agencies can start with when implementing ERM:

- Recommended agencies start with leadership and governance and establish an accountable lead to coordinate ERM implementation and leverage enterprise level governance.
- Integrate these efforts by putting in place a senior management council, senior assessment team or other similar oversight body.
- Assess GAO standards coverage and identify gaps.
- Develop an inventory of risk management activities and internal control assessments and leverage those activities.

BREAKOUT SESSION: ERM IN PROCUREMENT — NOT A NEW CONCEPT

Panel Moderator: Howard Campbell, Dir., IBC, a DBS Company

Panelists: Will White, Dir., Risk Management and Assurance, DHS; **Hyosun K. Ro,** Dir., Oversight and Pricing Branch, DHS; **Eileen Klase,** Oversight and Pricing Branch, DHS; and **Cory Baumhardt**, Financial Analyst, U.S. Department of Transportation (DoT)

Concept 1: Implementing ERM from a procurement perspective

Baumhardt explained that DoT is at the beginning stages of implementing an ERM program, but multiple risk management activities already exist. According to Baumhardt, the CFO office within DoT has a risk management and internal control process in place that recently moved toward a risk-based approach, utilizing qualitative and quantitative factors. Baumhardt highlighted the need for DoT to find ways to move away from stove piped approaches and views ERM as a valuable process moving forward.

White does not believe there is a one-size-fits-all approach to ERM; rather, it is a framework that is to be adapted to a particular organization's environment. The key is to understand what ERM can do for an agency and then mirror-up the organization's approach to align with the environment. The governance structure is the most important aspect of ERM, and liaisons from all avenues are needed to properly facilitate ERM. Risk concepts are not new; however, the new concept is the idea of putting an umbrella over it all to make it enterprise-wide. White is currently working with DHS leadership to move from a segmented internal controls and risk assessment process to a holistic and consistent framework.

The panel pointed out that ERM all rolls up to leadership and they take action from a holistic perspective and consider the risk involved.

Concept 2: Procurement best practices related to ERM

Klase explained that the goals of DHS through procurement are to support good business decisions and comply with relevant laws and regulations. Klase focused on three main risks within procurement in DHS:

- Not using agency-wide contract vehicles;
- Not facilitating competition; and
- An unmotivated workforce.

In terms of dealing with these risks, DHS conducts procurement oversight reviews in an attempt to identify cost savings, minimize redundancies and increase economies of scale. DHS monitors competition and rates through Federal Procurement Data System (FPDS) reviews and research. By utilizing a tool that leverages FPDS data, DHS can analyze whether procurements were properly competed. DHS monitors the achievement of professional certifications and monitors the graduation rate of a development program within DHS to analyze the motivation of the DHS workforce.

Ro made the case that there are inherent risks when spending money and said her office used to be more compliance-focused but is moving to a more internal controls and process-level analysis in an attempt to identify systemic issues. Ro identified several processes her office performs over procurement to assess risk. Through the procurement oversight program, the head of the contracting activity conducts self-assessments, on an annual basis, of its procurement functions. The results of these assessments are reported to the chief procurement officer. Additionally, DHS conducts acquisition plan reviews in which if a procurement exceeds a specific dollar threshold, the procurement file is reviewed by the chief procurement officer. DHS also conducts operational status reviews where FPDS data and metrics are used to analyze procurement health assessments, identify metrics in coordination with strategic plan objectives, and to identify and manage risks. However, the challenges with using FPDS data is that the contracts have already been executed.

Ro shared that DHS performs oversight reviews of procurement operations at each component. These tri-annual procurement reviews are conducted to assess compliance and controls. In addition, on an annual basis, specific topic reviews are conducted based on known concerns and new trends. Once fieldwork is completed, findings are discussed with process owners and corrective action plans are completed, as needed.

INTERNAL CONTROL OVER REPORTING (APPENDIX A) PREVIEW

Panel Moderator: Mark Reger, Deputy Controller, OMB

Panelists: Dan Kaneshiro, Policy Analyst, OMB; and **Michael Landry,** Policy Analyst, OMB

This session shared expected updates and key changes to Circular A-123 Appendix A, Internal Control Over Reporting — originally named, Internal Control Over Financial Reporting.

Concept 1: OMB Circular A-123 structure

- From the Integrity Act to the Green Book, reporting requirements have always expanded beyond financial reporting. Appendix A has been expanded to address internal control over internal financial reporting and internal and external non-financial reporting. The changes are an expansion on the concepts already in place for external financial reporting.
- Under the current Circular A-123 structure, Appendix A is co-mingled with the overarching circular. The forthcoming update will re-name Circular A-123 and make Appendix A a stand-alone document.
- Modifications will expand internal control standards beyond traditional areas and introduce concepts based on COSO and the GAO Green Book.

Concept 2: OMB Circular A-123, Appendix A Internal Control Over Reporting

- The scope of internal control over reporting has expanded into two concentrations, external and internal, with four objectives 1) external financial reporting objectives; 2) external non-financial reporting objectives; 3) internal financial reporting objectives; and 4) internal non-financial reporting objectives. **Figure 3** provides examples.
- Agencies will need to ask themselves what assurances and controls exist around the collection of data, data integrity and tracking information between procurement, grant, and financial systems.
- The updated Appendix A will specify at a higher level, the objectives and auditors will be asking about how agencies confirm data is reasonable and accurate. Ideally this improvement will lower risk and allow agencies to focus less time on external reporting.

> **"Don't let perfect get in the way of good enough."**
>
> —Mark Reger, Deputy Controller, OMB

- Appendix A also provides a new way to look at the data that is being reported and provides a discipline to assure that the universe of transactions is complete and relatable, as defined by required attributes.
- Internal control examples that are being considered for review in the general areas under Appendix A include process controls and system controls.
  - Process controls include policy and procedures; controls over human capital (e.g., training performance measures tied to data quality, etc.); and oversight of customer, stakeholder, and management reviews.
  - System controls include access controls; warnings and error checks (e.g., edit checks, override limits, etc.); and case history (e.g., audit trail, back-up data, etc.).

Figure 3: Internal control over reporting examples

External Financial Reporting Objectives	Internal Financial Reporting Objectives
■ The President's budget ■ Agency Financial Report (AFR) ■ www.USAspending.gov (financial data)	■ Financial Reports used to develop the AFR ■ Component/division reports
External Non-Financial Reporting Objectives	**Internal Non-Financial Reporting Objectives**
■ Internal control reviews ■ Custody of assets ■ www.USAspending.gov (non-financial data)	■ Benchmarking ■ Staff/asset utilization ■ Customer satisfaction metrics

THANK YOU TO OUR 2016 FORUM SPONSORS

Forum Co-Chairs

EY

KEARNEY& COMPANY

Platinum Sponsors

Cotton& Company
Answers Questioned

Deloitte.

Grant Thornton

ibc
A DBS COMPANY

KPMG

Gold Sponsors

accenture
High performance. Delivered.

AOCSolutions
Federal Financial Management Division

Castro& Company
Auditors ✓ Advisors

CGI

CliftonLarsonAllen

COHN REZNICK

Crowe Horwath

Franklin& Turner
Consultants and Certified Public Accountants

KGS

LMI

MORGANFRANKLIN CONSULTING

pwc

tfc

WILLIAMS ADLEY
Confidence Earned

the INS and OUTS of REPORTING

Box-checking

Focus solely on compliance

Over-engineering

Answering only the question asked

Repeating mistakes

Using jargon with multiple meanings

Expedited, one-time execution

"This isn't about checking a box — it's about assessing risks, knowing that the process encourages — demands — we look at things differently."

—Mark Reger, CPA, Deputy Controller, OMB

"We're working to tailor policy, agency-by-agency, so it's not a compliance exercise but works with what's in place."

—Dustin Brown, Deputy Asst. Dir. for Management, OMB

"We're offering flexibility in Circular enforcement because we realize we can't mandate things that should be agency-specific… It's important to show oversight restraint."

—Mark Bussow, Policy Analyst, OMB

"There's that old mantra, 'Only tell the auditors exactly what they ask,' — that wouldn't work well here."

—Eric Rasmussen, CGFM, CPA, Partner, KPMG, LLP

"We need to communicate *with* each other rather than *to* each other — that's only possible when using a set of well-defined terms."

—Ann Ebberts, AGA CEO

Thoughtful analysis

Focus on performance

Flexibility

Open, candid communication about risk

Learning from mistakes

Using an agreed-upon common language

Deliberate, ongoing and evolving way of doing business

OUTS of ERM

Excerpted from *Journal of Government Financial Management*, summer 2016; vol.65, no.2

CULTURE

OUT	IN
Blaming, scapegoating and working alone	Collaboration and teamwork
Single risk ownership	Shared ownership of risk and problems
Risk elimination	Risk review and management
Controls are only financial or within silos	Controls used across disciplines; taking down silos
Hiding problems	Socializing risks and building trust
Responsibilities assigned from the top, down	Shared responsibility among all team members
Budget-dictated	Mission-driven

"Leading ERM efforts is not about the person's title. This is about who within the organization has the ability and gravitas to pull this off. This is bigger than the CFO community."

—Mike Wetklow, CGFM, CPA, DCFO, NSF

"Over the past 25 years, the CFO community has proven not only are internal controls important, they should be expanded beyond the CFO community."

—Dave Mader, Controller, OMB

"ERM is about building relationships and trust."

—Cynthia Vitters, Sr. Advisor, ERM, OMB

"It's absolutely critical to have the right tone at the top — and also the right mood in the middle and among the boots at the bottom. Everyone has a very big role."

—Sheila Conley, CPA, DCFO, HHS

www.agacgfm.org