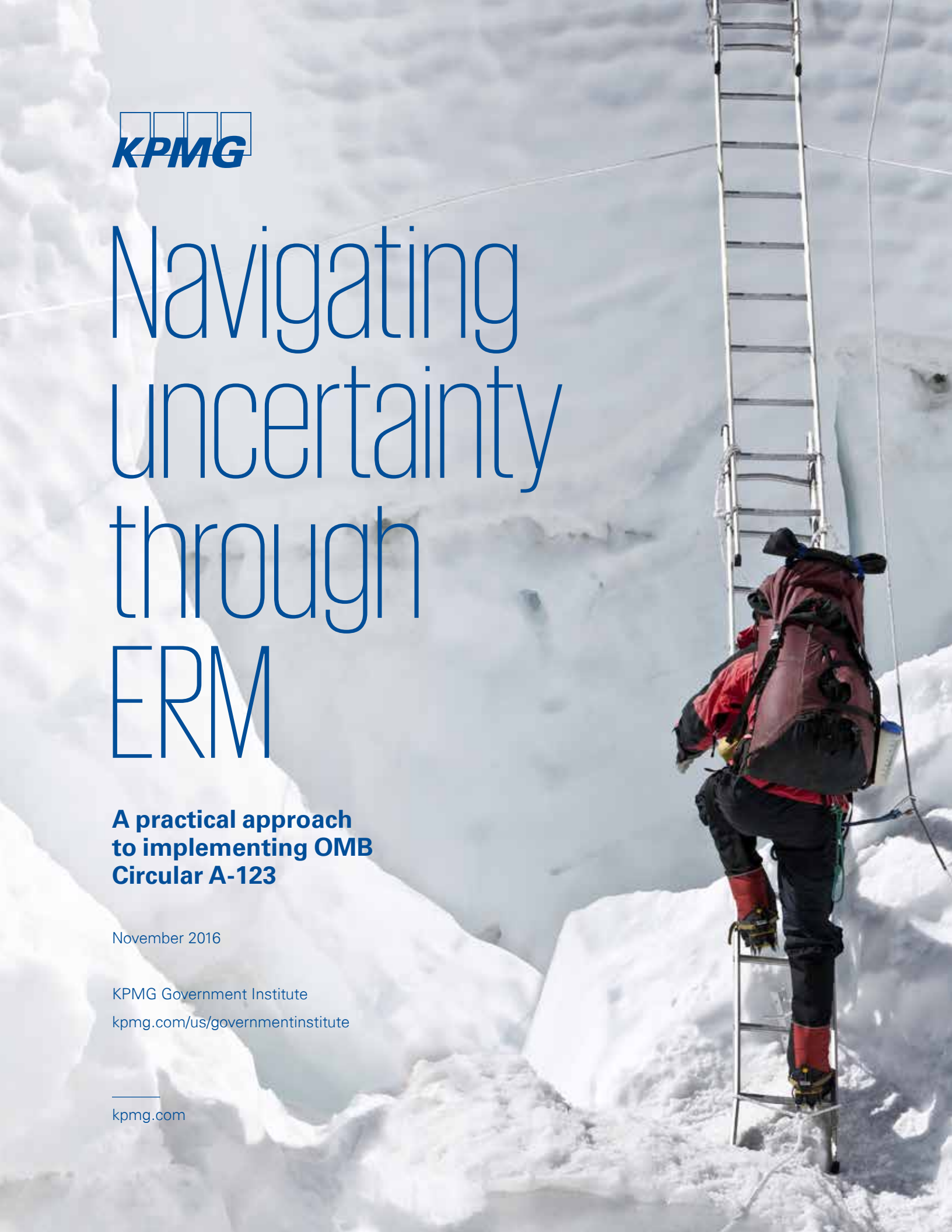


Navigating uncertainty through ERM

A practical approach to implementing OMB Circular A-123

November 2016

KPMG Government Institute
kpmg.com/us/governmentinstitute

kpmg.com

Contents

The KPMG Government Institute was established to serve as a strategic resource for government at all levels, and also for higher education and non-profit entities seeking to achieve high standards for accountability, transparency, and performance. The Institute is a forum for ideas, a place to share leading practices, and a source of thought leadership to help governments address difficult challenges such as performance management, regulatory compliance, and fully leveraging technology.

Visit www.kpmg.com/us/governmentinstitute

About the authors

Jeffrey C. Steinhoff is the managing director of the KPMG Government Institute, established in 2009, following his retirement from the Government Accountability Office (GAO) after a 40-year federal career. Jeff served as Assistant Comptroller General of the United States for Accounting and Information Management and managing director for Financial Management and Assurance. He led GAO's largest audit unit, with responsibility for oversight of financial management and auditing issues across the federal government. Included were establishment of the *Standards of Internal Control in the Federal Government* (Green Book) and assessments of internal control under the Federal Managers' Financial Integrity Act of 1982 (FMFIA) and Office of Management and Budget (OMB) Circular A-123. Jeff worked closely with Congress on the enactment of FMFIA, led GAO's oversight of FMFIA for 25 years, and testified before Congress and the SEC on internal controls. He is widely published and one of the authors of the 2008 *Managing the Business Risk of Fraud: A Practical Guide*, and the *Fraud Risk Management Guide*, published by Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Association of Certified Fraud Examiners in 2016. Jeff is an elected fellow of the prestigious National Academy of Public Administration and past national president of the Association of Government Accountants (AGA).

Laura A. Price is a partner and Risk Consulting leader in KPMG's Federal Advisory practice. In this role, she not only assists federal agencies but also is involved in the development and leadership of KPMG's broader Risk Consulting practice. Laura currently directly serves clients in the Defense and Intelligence practices, and has worked across all sectors of the federal government as well as state and local government. Her responsibilities over almost three decades include risk management and risk optimization; internal controls, including implementation of Circular A-123 and the Green Book; information technology portfolio analysis and information protection; activity-based costing; alternatives analysis; forensic services; business-process improvement; and legal and regulatory compliance. Laura is also an executive fellow of the KPMG Government Institute and coauthored, with Jeff, *The KPMG Executive Guide to High-Performance in Federal Financial Management*, as well as two articles in the AGA *Journal of Government Financial Management* (AGA *Journal*) addressing the federal government's human capital challenge and another article on high-performing finance organizations. She is also a coauthor of a summer 2016 AGA Journal article, with Jeff, Tom Cocozza, and Tim Comello, *Ten Steps to Sustainable Enterprise Risk Management* which was a principle source for the concepts in this white paper.

Thomas A. Cocozza is a director in KPMG's Federal Advisory practice and a fellow of the KPMG Government Institute. He has over 25 years of experience in areas such as financial and program management, risk management and internal controls, business process redesign, healthcare (including program integrity for the Affordable Care Act), information technology, operations, policy, program evaluation, strategic planning, mergers and acquisitions, corporate finance, and budgeting. Tom has developed strategy, financial management, and information technology solutions in federal and commercial organizations. He has deep experience in federal grants policy development and implementation as a charter member of OMB's Office of Federal Financial Management when it was established pursuant to the Chief Financial Officers Act of 1990. In addition to coauthoring the aforementioned summer 2016 AGA Journal article, Tom's 2011 article, "Making the Case for an Enterprise Integrity Solution," was published in the AGA *Journal*, and his article, "Balancing Risk and Performance," was published in the *Healthcare Financial Management Journal* in October 2008.

Introduction

In our everyday lives, we all face uncertainty. It is how we manage uncertainty that matters. We all accept risks. What matters is deciding how much risk to accept and when. Government is no different. It faces continuous and changing uncertainty and must make informed trade-offs in the public interest between risks and rewards.

Government is at a crucial juncture. Public confidence and trust have fallen appreciably,[1] and its value and role are being questioned. Demands on resources remain high, with growing public expectations and unmet needs such as rebuilding the nation's infrastructure. The long-term fiscal future is unsustainable[2] and becoming ever-more challenging with the passage of time. While certainly not a panacea for these formidable challenges, how government manages risk can help improve delivery of government programs and operations and public perception about the role and performance of government, while reducing costs and demands for future resources. Effective risk management protects and enhances value as an integral management tool.

In 1982, the Federal Managers' Financial Integrity Act (FMFIA)[3] dramatically changed the direction of risk management in the federal government from primarily an accounting and financial reporting orientation to broad consideration of program, operational, and administrative risks and controls. While there has been important progress, federal agencies continue to experience sudden and significant management breakdowns that only further undermine public confidence. Also, there are legitimate questions about whether there is a proper balance between risk and control, such that, in considering the risk impact and likelihood of occurrence, some areas are over controlled, while others are under controlled.

Risk management has now taken another dramatic turn with the most significant revision in over 30 years to Office of Management and Budget (OMB) Circular A-123,[4] which prescribes the FMFIA assessment and reporting requirements. From the July 15, 2016 transmittal of the revised Circular A-123: *"The Administration has emphasized the importance of having appropriate risk management processes and systems to identify challenges early, to bring them to the attention of Agency leadership, and to develop solutions. To that end, the Office of Management and Budget (OMB) is updating this Circular to ensure Federal managers are effectively and efficiently managing risks an Agency faces toward achieving its strategic objectives and arising from its activities and operations. These expanded activities reinforce the purposes of the Federal Managers' Financial Integrity Act (FMFIA) and the Government Performance and Results Act Modernization Act (GRPAMA)[5], and support the Administration's commitment to improve the efficiency and effectiveness of Government."*

"The policy changes in this Circular modernize existing efforts by requiring agencies to implement an Enterprise Risk Management (ERM) capability coordinated with the strategic planning and strategic review processes established by GPRAMA and the internal control framework required by FMFIA and Government Accountability Office (GAO)'s Green Book. This integrated governance structure will improve mission delivery, reduce costs, and focus corrective actions towards key risks."

In this way, federal agencies are being challenged to identify and focus on the most important risks through the aperture of an enterprise lens across management stovepipes and organizational boundaries. The changes in Circular A-123 can be described as transformational to the program and operational practices and culture of federal agencies.

In addition, in September 2014, GAO's *Standards for Internal Control in the Federal Government* (Green Book),[6] which establish the underlying standards that undergird

1. See http://www.people-press.org/2014/11/13/public-trust-in-government/ and http://www.gallup.com/poll/183605/confidence-branches-government-remains-low.aspx.
2. GAO "Fiscal Outlook: Federal Fiscal Outlook" (http://www.gao.gov/fiscal_outlook/federal_fiscal_outlook/overview).
3. Public Law 97-255, September 8, 1982 (https://www.whitehouse.gov/omb/financial_fmfia1982).
4. See https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf.
5. See https://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf.
6. GAO-14-704G, September 2014 (http://www.gao.gov/assets/670/665712.pdf).

FMFIA, were updated for the first time since 1999. The 2014 Green Book broadened control concepts through adoption of 17 new principles, consistent with private sector principles.[7] Included is an increased emphasis on fraud risk management, which is similarly prescribed in the revised OMB Circular A-123.

The evolution of Circular A-123 represents growing maturity in how federal agencies will address risk management going forward and an opportunity for agencies to gain greater value from their management processes and systems. There will be a natural period of adjustment given the transformational nature of the revisions. The status quo can be difficult to change, much less rapidly change. This is especially true in federal large agencies with widely diverse missions and operations, deeply-rooted program and operating cultures and ways of doing business, and many wide and diverse stakeholders.

It will also be imperative to find the right balance in establishing the level of management control to address risk. Think of policies, procedures, and operating systems as investments that help ensure that what the organization wants to have happen in fact happens, and what it wants to avoid is avoided. In leading organizations, ERM is anchored in a documented risk appetite, which is developed by management and shared with stakeholders such as the Congress. From Circular A-123: "*Federal managers must carefully consider the appropriate balance between risk, controls, costs, and benefits in their mission support operations. Too many controls can result in inefficiencies, while too few controls may increase risk to an unacceptable level.*"

Given the transformative nature of the changes to Circular A-123, as well as the Green Book, the KPMG Government Institute developed this white paper. Our objectives are to provide a snapshot of these changes and, more importantly, context into what is expected and why, and insights into implementation strategies. We highlight 10 critical elements for consideration in successfully implementing ERM programs. While developed for federal agencies, the basic principles and concepts would apply as well to state and local governments and higher education and not-for-profit entities. Our perspectives are based on first-hand knowledge from working with government agencies and private sector companies in the U.S. and globally and on secondary research into leading ERM practices. The authors, who are highlighted in the "About the authors" section, have decades of experience with respect to ERM, Circular A-123, and the Green Book.

7. Committee of the Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control – Integrated Framework,* 2014 (http://www.coso.org).

A snapshot of the changes to OMB Circular A-123 and GAO's Green Book

As defined in Circular A-123:
"ERM as a discipline deals with identifying, assessing, and managing risks. Through adequate risk management, agencies can concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events. … Risk management is a series of coordinated activities to direct and control challenges or threats to achieving an organizations goals and objectives. … ERM is an effective Agency-wide approach to assessing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than by addressing risks only within silos."

Also, from Circular A-123:
"ERM reflects forward-looking management decisions, balancing risks and returns so an Agency enhances its value to the taxpayer and increases its ability to achieve its strategic objectives."

While OMB Circular A-123 and the GAO Green Book have evolved over the past three decades, today, federal agencies face transformational change in the application of the concepts embedded in FMFIA. What do these changes mean to the federal government, as well as its business partners and stakeholders?

What is ERM?

ERM is premised on making choices and finding the right balance between risk and reward for the organization. It can be as simple as vigilance over what may cause management to lose sleep, or not want to see on the news or in blogs about their agency. But done correctly, it is much more complex, with the potential for improved mission effectiveness and efficiency and lower cost by protecting and enhancing value.

This is especially true for public entities, which can have an extensive and diverse array of stakeholders and vast webs of stand-alone systems and operations that are not integrated.

ERM is a tool to identify risks and help reduce their impact and likelihood of occurrence to an acceptable level consistent with the organization's risk appetite. The risk appetite defines management's tolerance for loss or negative results. Integral to ERM is risk mitigation – a decision to accept, avoid, reduce, and/or share risk. Simply put, ERM facilitates what the organization wants to make sure happens and happens well, and helps avoid what it wants to avoid, especially unwelcome surprises.

Management policies, procedures, and systems used to execute missions and operations and manage risks are investments. As with any investment, they need to be maintained and periodically reassessed to (1) protect and enhance value in line with mission goals and strategic objectives and (2) address current and emerging risks, while eliminating unneeded red tape. ERM supports this reassessment.

The revised OMB Circular A-123 in a nutshell

Formerly titled, *Management's Responsibility for Internal Control*, with the July 15, 2016 revision, Circular A-123 has been retitled, *Management's Responsibility for Enterprise Risk Management and Internal Control*.[8] As OMB stated in releasing the revised Circular A-123: "*The Administration has emphasized the importance of having appropriate risk management processes and systems to identify challenges early, to bring them to the attention of Agency leadership, and to develop solutions.*"

Based on the United Kingdom's *Management of Risk – Principles and Concepts* (Orange Book),[9] Circular A-123 now requires the integrated management of risk at strategic, program, and operational levels. In this way, the various organizational levels support each other and there is a holistic view of risks. OMB is requiring a direct linkage to the agency mission, goals, objectives, and strategy. Viewing ERM under the umbrella of governance and internal control as an integral part of ERM, as required in the revised Circular A-123, reinforces the relationship to program and operations management. An important distinction is that, while interrelated, ERM and internal control are not synonymous. Internal controls are tools to help manage risk and perform missions and operations.

The revision to Circular A-123:

- Introduces guidance on ERM and its application in the federal government
- Links ERM to strategic planning and performance reporting under GPRAMA and OMB Circular A-11, *Preparation, Submission, and Execution of the Budget* (Part 6, sections 230 and 270.24 to 270.28)[10]
- Adopts concepts and guidelines based on the Committee of the Sponsoring Organizations of the Treadway Commission[11] (COSO) *Internal Control – Integrated Framework*[12]
- Describes the relationship between ERM and internal control
- Encourages agencies to establish a risk management council (RMC) or a similar entity focused on ERM "*to provide governance in overseeing the establishment of an agency's risk profile, the regular assessment of risk, and the development of appropriate risk mitigation*"
- Provides implementation guidance for the 2014 GAO Green Book
- Establishes minimum requirements for corrective action plans, emphasizing root cause analysis, accountability, and collaboration with agency inspectors general (IG)

8. See https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf. Also, see OMB Circular A-11, *Preparation, Submission, and Execution of the Budget,* sections 270.24 to 270.28, July 15, 2016 (https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a11_2016.pdf).
9. United Kingdom, HM Treasury, October 2004 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf).
10. See https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a11_2016.pdf.
11. COSO is a joint initiative of five organizations (American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Federal Executives International (FEI), Association of Accountants and Financial Professionals in Business (IMA), and Institute of Internal Auditors (IIA)) dedicated to providing thought leadership through the development of frameworks and guidance on ERM, internal control and fraud deterrence (http://www.coso.org/).
12. See footnote 7.

— Requires risk reporting to provide a risk-based approach and balance the emphasis between the program, operational, reporting, and compliance objectives of internal control

— Increases the focus on fraud risk management

The 2014 Green Book

In a 2013 update of its *Internal Control – Integrated Framework*, COSO introduced 17 new principles related to the five longstanding components of internal control: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communications, and (5) monitoring.[13] In 1999, the Green Book adopted these five components. The 2014 Green Book adopted the 17 COSO principles, as shown in Appendix 1. Included is principle 8: "*Management should consider the potential for fraud when identifying, analyzing, and responding to risks.*"

The 2014 Green Book also includes attributes of internal control tied to each of the 17 principles, as well as related documentation requirements. Attributes are not standards or requirements and, as GAO cautioned, do not prescribe how agency management should design, implement, and operate its internal control system. A more apt description would be that attributes represent benchmarks or leading practices. GAO stressed that: "*Management has a responsibility to understand the attributes and exercise judgment in fulfilling the requirements of the standards.*"[14] In 2014, the length of the Green Book went from 20 to 80 pages. Agencies should fully expect that auditors will use the attributes and additional detail in the Green Book as criteria in evaluating management's stewardship over internal control and risk management.

A broader adoption of the Green Book by organizations receiving federal funding, such as the over $500 billion in annual federal grants, can help address the inherent risk to the federal government when federal funds are administered by other parties. From the forward of the Green Book: "*The Green Book may also be adopted by state, local, and quasi-governmental entities, as well as not-for-profit organizations, as a framework for an internal control system. Management of an entity determines, based on applicable laws and regulations, how to appropriately adapt the standards presented in the Green Book as a framework for the entity.*"

To complement the Green Book's specific focus in principle 8 on fraud risk management, in July 2015, GAO issued "*A Framework for Managing Fraud Risks in Federal Programs*" (Fraud Risk Framework).[15] GAO defines fraud risk management as the "*control activities to prevent, detect, and respond to fraud, with emphasis on prevention and mitigation.*" Based on leading practices, GAO's Fraud Risk Framework includes four components.

1. Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
2. Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
3. Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
4. Evaluate outcomes using a risk-based approach to adapt activities to improve fraud risk management.

(See Appendix 2 for additional details on the components of GAO's Fraud Risk Framework.)

In addition, in September 2016, COSO, together with the Association of Certified Fraud Examiners, issued the *Fraud Risk Management Guide*.[16] This guide is intended to serve as "best practices guidance" in implementing COSO principle 8 on fraud (and thereby relates to Green Book principle 8).

13. See footnote 7.
14. GAO-14-704G, September 2014 (http://www.gao.gov/assets/670/665712.pdf) See footnote 6.
15. "A Framework for Managing Fraud Risks in Federal Programs," GAO-15-593SP, July 2015 (http://www.gao.gov/assets/680/671664.pdf).
16. *Fraud Risk Management Guide,* Committee of Sponsoring Organizations of the Treadway Commission (COSO), September 28, 2016 (http://www.coso.org/documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf).

Incorporating fraud risk management in ERM

Large federal benefit,[17] procurement, and disaster assistance programs are particularly attractive targets to fraud perpetrators. Recognizing the criticality of combating fraud and preserving integrity in government agencies and programs, OMB incorporates fraud risk management as an integral component of ERM. The revised Circular A-123 cites Green Book principle 8 and states that managers should adhere to the leading practices in GAO's Fraud Framework.[18]

In addition, the Fraud Reduction and Data Analytics Act of 2015 (Public Law 114-186, June 30, 2016) requires OMB to establish guidelines for federal agencies to establish financial and administrative controls to identify and assess fraud risks and design and implement control activities in order to prevent, detect, and respond to fraud, including improper payments.[19] The guidelines must incorporate the leading practices identified in GAO's Fraud Risk Framework.[20]

Consistent with ERM, fraud risk management is anchored by management's risk appetite and governed by policies that articulate goals, objectives, roles, responsibilities, strategies, and tactics specific to fraud risk. Also, consistent with ERM, fraud risk management should be an integral part of all organizational processes and daily decision-making and should be systematic, structured, timely, dynamic, iterative, forward looking, and responsive to change.

Agency IGs play an important role in assessing fraud risk controls in operation, detecting and investigating fraud, and making recommendations to management on corrective actions to address identified fraud risks. At the same time, the Green Book makes clear that agency management and staff are the first line of defense. An essential element is management's continuous, day-to-day monitoring and evaluation to ensure control activities are operating as intended and timely action is taken to remediate identified breakdowns and weaknesses.

Fraud risk goes far beyond monetary considerations. Qualitative factors such as impacts on mission and program delivery, national security, and public health and safety can be the most important considerations in the government environment. For example, the purchase of defective or substandard military equipment used by soldiers in combat would be a far more serious concern than if the government was fraudulently overbilled for combat equipment that fully met all military combat standards.

Circular A-123 ERM development and implementation deadlines

OMB recognized that *"Federal agencies have diverse missions, and are at different levels of maturity in terms of their capacity to fully implement ERM."* OMB expects agencies to refine and improve their approach for developing risk profiles and implementing ERM each year.

As stated in Circular A-123:

- *"This guidance recognizes that not all components of an ERM process are fully operational in the initial years, and agency leadership must set priorities in terms of implementation."*
- *"Most agencies should build their capabilities, first to conduct more effective risk management, then to implement ERM rating those risks in terms of impact, and finally building internal controls to monitor and assess the risk developments at various time points. To complete this circle of risk management the Agencies must incorporate risk awareness into the agencies' culture and ways of doing business."*

Circular A-123 calls for the development of ERM maturity models. Also, as shown in Figure 1 below, Circular A-123 includes the following ERM development and implementation deadlines through September 15, 2017.

17. For example, Medicare, Medicaid, and other government health care programs are prime targets. A 2012 study pegged health care fraud nationally at a midpoint of 6.7 percent, with an upper range of 10 percent (http://healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_72.pdf and http://www.economist.com/news/united-states/21603078-why-thieves-love-americas-health-care-system-272-billion-swindle). The Federal Bureau of Investigation characterizes health care fraud to be in the tens of billions of dollars annually (FBI *Health Care Fraud* (https://www.fbi.gov/about-us/investigate/white_collar/health-care-fraud).
18. Circular A-123 also cites as additional guidance the Association of Government Accountants (AGA) *Fraud Prevention Tool Kit.*
19. See https://www.govtrack.us/congress/bills/114/s2133.
20. See http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2016/fraud-reduction-act.pdf.

Figure 1: ERM development and implementation deadlines

Deliverable	Due Date – No later than	Description
ERM Implementation Approach	*As soon as practicable, prior to June 2017 Initial Risk Profile deliverable*	Agencies are encouraged (not required) to develop an approach to implement ERM, which may include: — Planned risk management governance structure — Process for considering risk appetite and risk tolerance levels — Methodology for developing a risk profile — General implementation time line and plan for maturing the comprehensiveness and quality of the risk profiles over time.
Initial Risk Profile	*June 2, 2017*	Agencies must complete their Initial Risk Profile in coordination with the agency Strategic Reviews. Key findings should be made available for discussion with OMB by June 2, 2017* as part of the Agency Strategic Review meetings and/or FedSTAT. The final determination on information to be shared with OMB will be provided in early 2017. This Initial Risk Profile will inform the development of each agency's new strategic plan and the President's fiscal year (FY) 2019 Budget.
Integration with Management Evaluation of Internal Control	*September 15, 2017*	For risks for which formal internal controls have been identified as part of the Initial Risk Profile in FY 2017, all agencies must present assurances on internal control processes in the FY 2017 Agency Financial Report (AFR) or the Performance and Accountability Report (PAR), along with a report on identified material weaknesses and corrective actions. Until an agency has fully implemented an ERM approach to risk management, it may continue to provide the existing risk assurance statements to their IG and/or public accounting firms, as appropriate.
Management Evaluation of Internal Control	*Annually by June 3*	No less than annually, all agencies must prepare a complete Risk Profile and include required risk components and elements required by this guidance. Chief Financial Officer (CFO) Act agencies, at a minimum, must complete their Risk Profile in coordination with the agency Strategic Review. For these agencies, key findings should be made available for discussion with OMB by June 3rd[21] as part of the agency Strategic Review meetings and/or FedStat. The final determination on information to be shared with OMB will be provided in advance of these discussions. The Risk Profile will help to inform changes to strategy, policy, operations, and the President's Budget.

Source: OMB Circular A-123, July 15, 2016

21. OMB Circular A-11, Part 6, is the authoritative policy guidance on deadlines for the Summary of Findings from agency Strategic Reviews, including the timing of submissions to OMB. (See https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s200.pdf.)

ERM Playbook

Supporting tools designed to help federal agencies meet the requirements of OMB Circular A-123 are included in the "*Playbook: Enterprise Risk Management for the U.S. Federal Government*" (ERM Playbook), issued by the federal Chief Financial Officers Council (CFOC) and the Performance Improvement Council (PIC) on July 29, 2016.[22] From the ERM Playbook transmittal letter, *"The Playbook guidance and accompanying appendices are tools designed to help government departments and agencies meet the requirements of the revised Office of Management and Budget Circular A-123. They are also designed to provide high-level key concepts for consideration when establishing a comprehensive and effective ERM program. The Playbook especially addresses the additional requirements included in Section II in A-123, which defines management's responsibilities related to ERM, to help departments and agencies make better decisions based on a more holistic view of risks and their interdependencies."*

The ERM Playbook includes guidance covering issues such as: (1) integrating ERM into management practices; (2) ERM basics, including common risk characteristics, ERM outcomes and attributes, and implementation maturity; (3) the ERM model; (4) the ERM implementation approach; (5) risk governance; (6) risk appetite statement; (7) developing a risk profile; and (8) GAO and IG engagement. The ERM Playbook is not authoritative or prescriptive and does not set standards.

22. See https://cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf.

Ten critical ERM implementation elements

The movement to ERM requires transformative ways of considering risk. Federal agencies will need to be more anticipatory and break down deeply-rooted cultural barriers that may inhibit the consideration of risks across agency components and between agencies. Incorporating ERM into the day-to-day management of an agency requires a disciplined approach that builds upon various attributes of leading organizations. We have identified 10 critical elements for a sustainable ERM implementation strategy in the federal government.

Government is not "home alone"

Government is certainly not alone with respect to ERM and can learn from others' experiences. The May 2013 results of a KPMG-sponsored global risk management survey,[23] conducted by the Economist Intelligence Unit (EIU),[24] showed that companies worldwide recognize they are at a turning point in needing even stronger capabilities to master and optimize risk management. The more than 1,000 C-suite executives surveyed reported they faced significant challenges in adopting ERM concepts.

Risk management was viewed as making a key contribution to the business, with 47 percent indicating it was essential for adding value, and another 34 citing occasional improvement through risk management. However, respondents saw the need to improve how they measure risk management's return on investment and how they communicate process, values, and effectiveness to key stakeholders. There was a general recognition of the need to integrate a holistic governance, risk, and compliance framework, which is in line with the revised Circular A-123 expectations.

The survey results below provide a window into the critical elements of an implementation strategy for federal agencies as they move forward in implementing the changes to Circular A-123 and the Green Book.

- Two-thirds of global respondents built ERM into strategic planning, which is required by Circular A-123. However, a third had not done so.
- Most respondents did not have a consistent way of assessing enterprise risk; thereby limiting the usefulness of the results.
- Most had a process to develop and aggregate their risk profile; another fundamental components of ERM. But, 20 percent reported having no process at all.
- Thirty-eight percent relied only on business-unit self-assessments. This is essentially what federal agencies have done in the past under FMFIA. While valuable, it can result in too narrow a focus and limit the ability to connect all the dots at the enterprise level.
- Almost half reported they had difficulties understanding enterprise risks. Without this understanding, ERM considerations have limitations and the risk of this becoming a paperwork exercise increases.
- Less than 44 percent believe they were effective at developing stakeholder understanding. This is especially important in government for which stakeholder expectations become the reality for agencies; whether it be the public, the President, or the Congress.
- Forty-two percent cited a lack of skills as an obstacle. In designating human capital management as one of 32 federal high-risk areas, GAO said: "*Mission critical skill gaps impeded federal agencies' efforts from cost effectively serving the public and achieving results*."[25]

23. KPMG International, "Expectations of Risk Management Outpacing Capabilities – It's Time For Action," May 2013 (https://portal.ema.kworld.kpmg.com/Adv/SG02/go_rc_lib/01/ExpectationsOfRiskManagementOutpacingCapabilitiesSurvey.pdf).
24. The EIU is an independent business within The Economist Group that is a sister organization to the well-known journal *The Economist*. EIU provides KPMG with a range of services that offer analysis, forecasts, and data for countries around the world in a consistent and comparable way to aid understanding of the environment of countries over time.
25. "HIGH-RISK SERIES: An Update," GAO-15-290, February 2015 (http://www.gao.gov/assets/670/668415.pdf).

There is a changing of the guard in the federal government with the long-awaited wave of employee retirements underway, which combined with other factors, threatens the ability to effectively recruit and engage staff.[26]

- Forty-three percent cited a weak link between risk management and compensation. In the federal government, this translates to organizational and personal incentives.
- Seventy-five percent had some way of assessing the return on investment, with 25 percent reporting they had no way of assessment. Being able to measure results, even those that are qualitative, provides information needed to help determine whether the program is working effectively and efficiently. If there is no return, or the return is negative or not within benchmarks for similar organizations, it may be time to reassess how the ERM program is structured. ERM should provide measurable value.

The "2015 Report on the Current State of Enterprise Risk Oversight: Update on Trends and Opportunities" (ERM Initiative), the sixth annual report in this series developed for the American Institute of Certified Public Accountants (AICPA), with almost 1,100 business respondents, had similar findings.[27] Of particular note to the challenge faced by federal agencies were the respondents that had not yet implemented ERM programs when asked, "*why not*?" Forty-seven percent believed "*risks are monitored in other ways besides ERM*." The report made the following observation: "*This strikes us as interesting and paradoxical, given the lack of risk oversight infrastructure discussed in prior pages of this report. It begs the question, so what processes are in place to help management and the board keep its eyes on emerging, strategic risks?*""

Critical elements of an ERM implementation strategy

Implementing an ERM program represents significant operational change and cultural transformation for federal agencies. As OMB stated in its memorandum to the heads of executive departments and agencies transmitting the revised Circular A-123: "*Successful implementation of this Circular requires Agencies to establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame. An open and transparent culture will result in the earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a more resilient government.*"

ERM has to be owned, understood, and implemented by everyone in the organization, starting at the top. Leaders will have to be motivated, and that motivation will have to be sustained since transformative change will not happen overnight and will transcend administrations. Risk management is a process that never ends in our daily lives or in organizations such as federal government agencies.

OMB Circular A-123 does not speak of the end game of ERM in terms of compliance with FMFIA and the GAO Green Book, but that effective risk management:

- Creates and protects value
- Is an integral part of all organizational processes
- Is part of decision making
- Explicitly addresses uncertainty
- Is systematic, structured, and timely
- Is based on the best available information
- Is tailored and responsive to the agency's evolving risk profile
- Takes human and cultural factors into account
- Is transparent and inclusive
- Is dynamic, iterative, and responsive to change
- Facilitates continual improvement of the organization

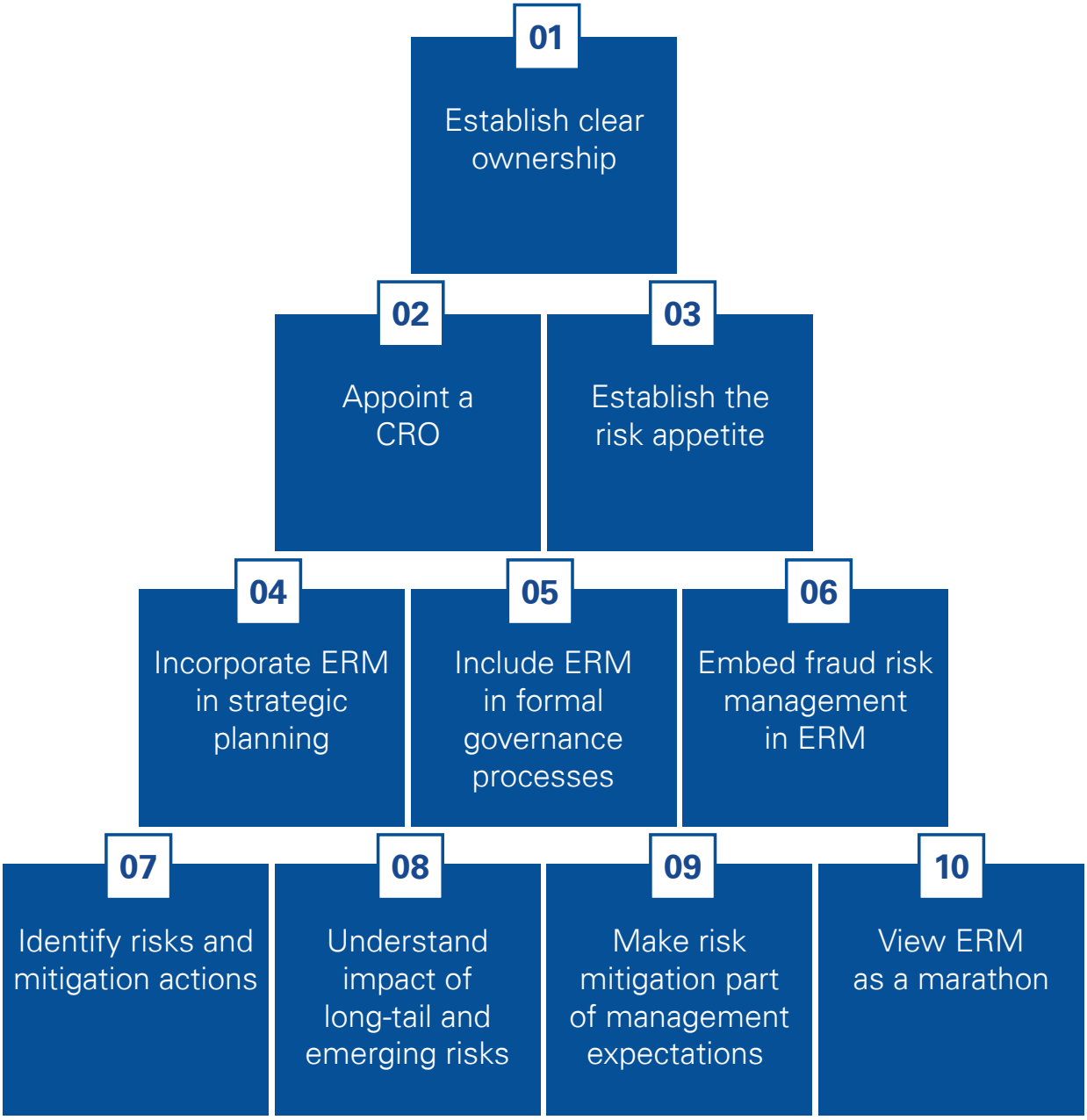
As further stated in Circular A-123, "*ERM reflects forward-looking management decisions, balancing risks and returns so an Agency enhances its value to the taxpayer and increases its ability to achieve its strategic objectives.*"

Before highlighting each element, for quick reference, here are KPMG's 10 critical elements for federal agencies.

---

26. "Making Human Capital Management a Strategic Business Priority in a Changing Financial Management World," by Corbin Neiberline, Howard D. Simanoff, Andrew C. Lewis, and Jeffrey C. Steinhoff, AGA *Journal*, Fall 2015 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2015/human-capital-management.pdf).
27. The report is based on research by the Enterprise Risk Management Initiative at North Carolina State University on behalf of the AICPA's Business, Industry, and Research Team to survey CFO's or equivalent senior executive positions in business on various characteristics ERM (https://erm.ncsu.edu/az/erm/i/chan/library/AICPA_ERM_Research_Study_2015.pdf).

KPMG's 10 Critical Elements of ERM Implementation



The following critical implementation elements can be adapted to an agency's needs and are meant to be considered in the context of Circular A-123 and the ERM Playbook and consistent with the Green Book standards. There may be other leading practices as well that agencies may wish to consider. Also, while they are listed 1 to 10, this does not mean that everything would be considered sequentially. Certain elements build off of one another; but many actions can be taken concurrently.

01 *Establish clear "ownership" by the agency's top leadership and cascade ownership down the organizational chain of command, so everyone understands their responsibility.*

Successfully implementing an ERM program is not about issuing a memorandum, sending an email to all staff, having a town hall meeting, or all of the above. The changes to Circular A-123 and the Green Book are transformative. Success may largely hinge on changing the organization's risk management culture. The risk culture – the human factor – is the heart and soul of ERM. This is never easy; especially in large federal agencies for which component organizations may have different missions and cultures. There must be a sense of urgency, clear, but realistic expectations, recognition for success, and accountability for failure.

Ownership by top leadership is paramount to success in federal agencies that generally have many priorities and perhaps limited capability to address everything on their plate. In organizations considered 'advanced' in implementing ERM, we have observed that senior management leads by example by making risk management a clear priority and driving appropriate risk management behavior.

Consider these questions to help gauge the ownership of agency top leadership:

- Is top management fully invested in the role of ERM and concepts that represent sound systems of internal control, so this commitment permeates through the organization and over time becomes embedded in the culture?
- Does top management instead view the changes in Circular A-123 and the Green Book as an unfunded requirement or new compliance exercise that is essentially the purview of the chief financial officer (CFO) and/or the IG?
- Does top management agree in concept with the value of moving ahead with ERM, but has higher priorities and is not willing to invest the time and effort in the program?
- Or do the changes to Circular A-123 and the Green Book not even make it to top management's radar screen?

The reality is that government agency top management is faced with many challenges, and everything cannot be a priority. This is not different from business. The 2015 ERM Initiative report noted that 42 percent of survey respondents viewed competing priorities as a barrier to ERM progress.[28] Also, within presidential administrations, and especially with a change of administrations, the mass turnover of top leadership adds an additional dimension that goes beyond the private sector experience.

Therefore, there will need to be a clear understanding of the costs and benefits of incorporating ERM concepts in the normal day-to-day program and operation management processes, as well as the mechanisms for effectively and efficiently doing so. On one level, top management commitment may seem like a relatively easy hurdle. But it may turn out to be the most difficult step in the process, especially when one considers the need to change the organizational culture by sustaining a high level of top management interest over time.

02 *Appoint an agency chief risk officer.*

Appointment of a chief risk officer (CRO) is a leading practice. OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*,[29] provides guidance on the role of a CRO, and some federal agencies have already appointed CROs. (See Appendix 3 for excerpts from Circular A-11 on the role of the CRO.)

For example, from Circular A-11: "…. *An effective enterprise risk manager …. Develops, manages, coordinates, and oversees a comprehensive system for proactively, identifying, prioritizing, monitoring, and communicating an organization's enterprise-wide risks. Such risks include relevant strategic, operational, financial, and programmatic barriers as well as, reputational risks that could interfere with an organization defined strategic objectives or performance goals.*"

In addition, the revised Circular A-123 discusses establishment of a RMC or a similar entity to support governance oversight of agencies' ERM programs. This places emphasis on the enterprise scope of the effort and can help break down barriers and build integration strategies.

28. See footnote 27.

29. OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget,* sections 270.24 to 270.28, July 2016, (https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a11_2016.pdf).

The responsibilities of managing risk, however, are not solely, or even primarily, the job of the CRO. Risk management must be shared throughout the agency and owned by everyone— from the highest levels of executive leadership to the program and operations delivery staff executing and supporting programs every day. The CRO, supported by the RMC, CFO, chief information officer, chief human capital officer, and other key leadership, should act as a facilitator, who helps pull everything together in support of the agency head and program and operations leadership.

Appointing a CRO sends a powerful signal that this is a top management priority. The CRO should be adequately empowered and have sufficient capabilities and resources to add value and make a measurable difference. In establishing this position, define the expected return on investment and monitor performance. Avoid this becoming window dressing by being very clear as to the expectations of the CRO and of program and operations leaders to support the CRO while in no way abdicating their own core ERM responsibility.

The 2015 ERM Initiative report noted that 32 percent of the almost 1,100 business survey respondents have designated a CRO or equivalent.[30] Financial service firms are most likely to do so at 56 percent. Also, 45 percent of respondents companies have a risk management committee that meets at least quarterly. Finally, 70 percent of the boards of the directors of the largest companies responding to the survey have formally assigned risk oversight responsibility to a board member.

03 *Establish the risk appetite, and make it part of day-to-day program and operations management.*

Establishing an agency's risk appetite is critical to ERM. Put simply, unless you know what your risk appetite is, there's no way to gauge whether you're taking too much risk or not enough risk protecting and enhancing strategic value. Many government organizations, as well as private sector companies, still view risk appetite solely as a line not to cross, but leading organizations use it to determine whether they can and should be taking more risk. Developing a clearly defined, top management endorsed risk appetite, and using this to both promote the right risk culture and take a harder look at the "upside" of risk-taking, are front and center of leading edge ERM practices.[31]

As defined in OMB Circular A123, risk appetite is: *"The broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives."*

As addressed in Circular A-123, in addition to an organization's risk appetite, COSO's ERM framework also includes consideration of the risk tolerance, which is defined as "…. *the acceptable level of variance in performance relative to achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of related objectives and aligns risk tolerance with risk appetite.*" The expectation is to translate the agency's overall risk appetite to specific programs and operations since the tolerance for risk may differ greatly within an agency.

In addition, the Green Book defines risk tolerance as: *"The acceptable level of variation in performance relative to the achievement of objectives…. Management defines the risk tolerance for defined objectives by ensuring the set levels of variation for performance measures are appropriate for the design of an internal control system."*

OMB and COSO also address the term "portfolio view of risk," which provides insight into all areas of organizational risk exposure. As stated in Circular A-123, a portfolio view results in *"increasing an Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment."*

Leading organizations carefully define their risk appetite and any related risk tolerances, communicate what they mean across the entity, and live by them day-to-day. They develop a common understanding of the why, what, who, and when. They also engage stakeholders such as legislators and the public, so there is a shared understanding of the risk appetite and no surprises.

The risk appetite reflects the agency's mission and strategy, including organizational objectives, strategic plans, and stakeholder expectations. Management is acknowledging a willingness and capacity to take on some level of risk and a tolerance for loss or reasonably quantifiable negative results. There is a recognition that attempting to set up costly, fail-safe systems to attempt to avoid all risk may not be not feasible or even necessary

30. See footnote 27.

31. "Enterprise risk management – Protecting and enhancing value," KPMG LLP, September 2016,

in all cases. The risk appetite is intended to help drive decisions based on relative priorities and the balance between mitigation and cost.[32] Also, reputational and other qualitative risks should always be a consideration.

Risk management alternatives and their relative costs – both quantitative and qualitative—are considered. Trade-off decisions are fact-based; meaning supported by analysis of costs, potential adverse impacts and benefits, and alternatives. In some areas, the cost of reducing risk may not be the primary consideration. For example, certain matters involving national and homeland security and public health and safety may have very little to no tolerance for risk, with cost not being a significant consideration.

Once the agency has established the risk appetite, everyone should be empowered to work within that framework, with the organization accountable for any adverse impacts. This does not mean agencies should not be concerned when avoidable problems arise. They should determine why and what could have been done differently. Also, agencies should periodically reevaluate their risk appetite, especially when there have been changes in the risk environment and/or in stakeholder expectations. Metrics and monitoring programs become important and are integral to making continuous, fact-based decisions as to the risk appetite.

If organizations or individuals exceed the risk appetite, they should be held accountable, unless there is a compelling reason for their actions, such as a national disaster or emergency. In this regard, Circular A-123 includes a section titled "Establishing Risk Tolerances in Disaster Situations." These decisions should be documented and shared with key stakeholders, as appropriate, so there are no surprises. Also, even in those cases, it is critical to consider alternatives to keep risk within the appetite established by management and to identify and follow up on any problems. Conversely, if organizations or individuals do not go far enough in accepting risk and retain processes that are not value added, top management should seek answers as to why they made that decision.

Establishing the risk appetite may start with management addressing fundamental questions, such as the two questions raised earlier: What do we lose sleep over? What do we not want to see on the news or in blogs? Appendix 4 contains 10 questions agencies may find helpful. While these are fundamental questions, and there are many others, they can help an agency better focus on the risk environment and address risk broadly across the enterprise. Ultimately, relationships between programs and operations and a view of external risks in conjunction with internal risks can provide a foundation for establishing the risk appetite.

Always remember that establishing the risk appetite is never 'one time and done.' The risk appetite has to be continually reassessed by management. If the organization is not doing so, it is exposing itself to unpleasant surprises.

04 *Incorporate ERM in strategic planning.*

Strategic plans guide federal agencies' programs, operations, and related priorities. They communicate top management's priorities to staff and stakeholders and are enterprise-wide as well and focused on programs and operations. They can be used to reinforce top management's priorities and provide a clear link between the theory of ERM and the application against strategic priorities.

Making this link in the strategic plan reinforces how integral ERM is to agency programs and operations. The goal should be for program and operations management to view ERM as their day-to-day responsibility, with the CRO, supported by the RMC, CFO, and others, a means of facilitating success through assistance and oversight. The ultimate goal is to embed ERM in the normal business processes and systems so that it becomes second nature and adds clear value. As highlighted earlier in Figure 1, OMB plans to use agency risk profiles, developed under Circular A-123, as part of agency strategic reviews and to inform development of strategic plans and the President's Budget.[33] In this way, ERM links directly to GPRAMA and OMB Circular A-11, Part 6, sections 230, *Agency Strategic Planning*, and 270.24 to 270.28, *Performance and Strategic Reviews*.

Strategic planning provides another opportunity to help identify and break down any organizational barriers standing in the way of effective and efficient ERM implementation. Eliminating organizational stovepipes and promoting enterprise partnerships between and among programs and operations are essential components to affecting meaningful cultural change and establishing value. This can present a significant challenge, especially in large organizations with a wide range of missions and constituencies, such as congressional authorizing and oversight committee and public-interest groups.

32. "Understanding and articulating risk appetite," KPMG Australia, Advisory, June 2008, (https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Risk-appetite-O-200806.pdf).

33. The first initial agency risk profiles are due no later than June 2, 2017, which would coincide with development of strategic plans and preparation of the President's 2019 budget.

Private sector companies face similar challenges with respect to linking ERM to strategic planning. The "2015 Report on the Current State of Enterprise Risk Oversight: Update on Trends and Opportunities" noted that "*48% believe that existing exposures are considered "mostly" or "extensively" when evaluating new strategic initiatives. But, 36% do no normal assessments of emerging, strategic, or industry risks*." Also, only 27 percent responded that their company boards of directors "mostly" or "extensively" reviewed the top risk exposures when discussing the strategic plan, and only 33 percent of organizations considered the risk appetite in the context of strategic planning.[34]

05 *Include ERM in the agency's formal governance processes.*

Circular A-123 establishes ERM as a component of agency governance. The governance process represents operating practices that help ensure programs and operations are working as intended and that day-to-day decisions and actions are consistent with risk appetite. In leading organizations, the ERM governance process includes:

Clear roles and responsibilities for ERM across the enterprise. Even in organizations that have a CRO, this will help reinforce the broad responsibility of program and operational management and staff for ERM. This is part of cultural transformation, whereby the responsibility for risk management must be broadly owned across the enterprise.

Well-designed policies and procedures to cover risk assessment, identification, categorization, and mitigation. Included would be sound methodologies to develop meaningful and consistent risk profiles across agency entities that enable the agency to then connect the dots and also understand the interrelated nature of risks. Each assessment should be viewed through the lens of whether it added value in managing risk across the agency. It should never be process for process sake.

In developing policies and procedures, the ERM Playbook guidance and accompanying appendices were designed to help agencies meet the requirements of Circular A-123 and provide high-level key concepts for consideration when establishing a comprehensive and effective ERM program.

Fact-based trade-offs between control and cost, alternatives, and the relative importance of risks associated with different programs and operations. OMB Memorandum-07-24, *Updated Principles for Risk Analysis,*[35] and OMB Circular A-129, *Policies for Federal Credit Programs and Non-Tax Receivables,*[36] provide guidance on risk management in several specialized areas including environmental, health, safety, credit programs, and non-tax receivables. Also, the Chief Financial Officers Act of 1990 (CFO Act)[37] calls for the systematic measure of performance and development of cost information, which are essential to fact-based trade-offs.[38] In addition, developing information for fact-based trade-offs would also support performance management under the Government Performance and Results Act of 1993 (GPRA)[39] and GPRMA.[40]

Documenting key judgments in a manner so management is not encumbered with mountains of documentation supporting decisions on the risk appetite and risk assessment to name just two areas. In the early years in particular, GAO found that FMFIA implementation was burdened by far too much process and a blizzard of paper supporting assessment and reporting.[41] There was not requisite focus on concrete results.

At the same time, management must document the rationale for its decisions. If the risk appetite is set at a certain level, why and what evidence supports the decision? COSO said it well in its Integrated Framework, controls "*cannot be performed entirely in the minds of senior management without some documentation of management's thought process and analysis… management would need to document significant judgments, how such decisions were considered, and how the final decisions were reached*."

34. See footnote 27.
35. See https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-24.pdf.
36. See https://www.whitehouse.gov/sites/default/files/omb/assets/a129/rev_2013/pdf/a-129.pdf.
37. Public Law 101-576, 104 Stat. 2838, November 15, 1990.
38. "The CFO Act Turns 20 Years Old: As We Blow Out the Candles, Where Are We Today and Where Do We Go From Here?" by Jeffrey C. Steinhoff and John R. Cherbini, AGA *Journal*, winter 2010 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/archive/cfo-act-anniversary.pdf).
39. Public Law 103-62, 107 Stat. 285, August 3, 1993.
40. Public Law 111–352, 124 Stat. 3866, January 4, 2011.
41. "FINANCIAL MANAGEMENT – Effective Internal Control is Key to Accountability," Statement of Jeffrey C. Steinhoff, Managing Director, Financial Management and Assurance, GAO-05-321T, February 16, 2005 (http://www.gao.gov/assets/120/111338.pdf).

Accountability and transparency for results to reinforce management's commitment and everyone's responsibility. Agencies should establish incentives for people to do the right thing; transparency to help assure they do the right thing; and effective accountability mechanisms if they don't do the right thing. Absent any of these three imperatives, successful implementation of an ERM program becomes more difficult.

Oversight and monitoring, whereby management is aware of performance against the risk appetite and risk tolerances on an ongoing basis. Metrics must be well-designed and information timely, reliable, and in useful formats to gauge performance and establish accountability for results. Performance metrics will need to be periodically reevaluated and adjusted accordingly based on any changes in expectations or performance shortfalls. Finally, they must be used by top management and cascaded throughout the agency.

Education to help avoid the 'lost in transition' syndrome and to emphasize that ERM does not represent a compliance exercise, but a way of doing business in the public interest. It will be especially important to translate the value to program and operational line-managers. They are integral to the success of this new paradigm, but may already feel overburdened and may not view this as their responsibility.

Everyone will not only have to understand "what" is required and "how" do it, but also "why" OMB has adopted ERM. It is imperative for staff at all levels to have the requisite context sophistication over the benefits and concepts at the foundation of ERM. Without context sophistication, there is an increased risk that organizations will go through the exercise of complying with ERM requirements without gaining the full range of benefits from an ERM program. If ERM primarily becomes a compliance exercise or is viewed as just a new way of talking about internal control assessments, an agency will simply not gain the benefits possible and may even introduce new risks.

Open communication so risks are quickly raised to the highest level necessary to timely address the problem and so lessons learned are widely shared. As stated in the revised Circular A-123: "*ERM is beneficial since it addresses a fundamental organizational issue: the need for information about major risks to flow both up and down the organization and across its organizational structures to improve the quality of decision-making. ERM seeks to open channels of communication so that managers have access to the information they need to make sound decisions.*"

People in the organization can be the best source of intelligence as to risks. But are they incentivized to come forward, or are they concerned about negative repercussions to their career, such as retaliation, if they do so? If staff at all levels feel constrained in any way, the agency will lose a valuable source of risk intelligence. OMB addressed this in Circular A-123 in stating that: "*Successful implementation of this Circular will require Agencies to establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame.*" In this regard, the National Business Ethics Survey (NBES) provides the U.S. corporate benchmarks on ethical behavior. The most current survey in 2013 found that 63 percent of those observing misconduct in private companies reported the misconduct, of which 21 percent said they faced some form of retaliation, which was viewed as a problem.[42]

Continuous reevaluation at the highest levels in the organization with respect to changes in the risk environment. ERM must be a continuous process. As stated earlier, it is not one and done where someone checks the box that the job has been completed. It must become part of the organization's management fiber that drives day-to-day decision-making and operations. The consideration of enterprise risk should be fundamental to management and not something added on to the process.

Involvement of stakeholders to help ensure everyone is on the same page. Work with stakeholders to develop approaches and tools to address common risks, whether it be benefit, credit or contract fraud; cybersecurity; identity theft; national or homeland security threats; public health and safety vulnerabilities; or public corruption. Collaboration and benchmarking should be a priority. Stakeholders include the Congress, the public, other federal agencies, state and local governments, contractors, auditors, and interest groups. Also, keep them apprised about the agency's ERM program and elicit their feedback and insights.

42. The 2013 NBES is the eighth in the series since 1994. Link to the 2013 NBES Executive Summary at https://www.ethics.org/research/eci-research/nbes/nbes-reports/nbes-2013.

Partnership with the IG to share intelligence on current, emerging, and long-tail risks and leading practices. Management owns risk management. The IG is an independent auditor/investigator, which under *Generally Accepted Government Auditing Standards*,[43] cannot make an agency management decision or perform a management function. This does not mean the IG has to be at such a degree of arm's length from agency management that it cannot share perspectives. Under *Government Auditing Standards,* IGs can provide routine advice and respond to questions, including sharing leading practices. The IG has a lot to offer in terms of leading practices related to ERM, including fraud risk management.

In this regard, from Circular A-123: "…. *agency managers, Inspectors General and other auditors should establish a new set of parameters encouraging the free flow of information about agency risk points and corrective measure adoption.*

Leverage the CFO, who brings valuable risk management capability and works across the agency. High-performing finance organizations are those that have moved far beyond the basic accounting, control, and financial reporting tasks that represent the "back room" of finance, to a role in regularly providing services and insights to program managers and in the agency's executive "board room" where decision support and strategic leadership occur.[44] CFOs can be invaluable in implementing sound ERM programs that add value.

Think of high-performing CFO organizations as operating in three areas of responsibility, or dimensions: (1) *Finance Operations,* by performing basic finance functions with a high degree of effectiveness and efficiency; (2) *Program Operations,* by supporting achievement of the agency's programs and operations with reliable, relevant, and timely financial information and analysis and effective and efficient internal controls and risk management; and (3) *Enterprise Operations,* by serving as a key member of the agency's senior leadership team.

ERM maturity models to be used as tools to continually assess the maturity and value of the ERM program and the supporting processes, considering the attributes of maturity across a continuum. The advanced level may not always be the target maturity at a particular point in time, especially when agencies are just beginning to adopt ERM. Rather, the target should reflect management's view on what is critical to successfully manage risk and the benefits it wants to achieve. In establishing a maturity model, there should be full recognition that stakeholders, including the public and the Congress, expect a high level of accountability and transparency over federal spending and operations.

There can be a variety of maturity models. What is important is that there is clear criteria that helps move the organization forward over time, so ERM becomes part of daily business operations and decision-making. The ERM Playbook includes the following five-step maturity model.

Level 1 – Nascent: Lacks formal ERM process; no basic communication or monitoring; risks addressed as they arrive; fails to anticipate potential risks.

Level 2 – Emerging: ERM roles and responsibilities are defined; governance established; risks are identified and assessed; rarely well prepared for unanticipated events.

Level 3 – Integrated: ERM program is endorsed by leadership; policies and procedures are in place for some activities; risks are shared across silos; occasionally well prepared for unanticipated events.

Level 4 – Predictive: ERM program is recognized by the whole organization; policies and procedures are in place for all activities; risks are identified and qualitatively assessed; periodically well prepared for unanticipated events.

Level 5 – Advanced: Risk discussion is embedded in strategic planning, capital allocation, and other processes and in daily decision-making. An early warning system is in place to notify management of risks above established thresholds; regularly well prepared for unanticipated events and have learned from past events to improve processes.

Maturity can be tied to key risk elements. Let's consider what a maturity model might look like for KPMG's critical ERM implementation element 3, *risk appetite*, and element 4, *strategic planning*, along a continuum of three levels of maturity—basic, mature, and advanced.

1. ***Basic***: There is a basic definition of the overall risk appetite and some formal consideration of risk in strategic planning.
2. ***Mature***: Risk appetite is clearly defined and understood across the agency and by stakeholders. Risk is a key aspect of strategic planning and used to support program and operational decisions at all levels of the agency.

43. See http://gao.gov/assets/590/587281.pdf.

44. *The KPMG Executive Guide to High Performance in Federal Financial Management*, KPMG Government Institute, June 2009 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/archive/ffm-executive-guide-final.pdf).

3. Advanced: Risk is integrated with strategic planning, and risk strategy includes use of sophisticated business intelligence tools, continuous dashboards, and robust scenario analysis. ERM is embedded in day-to-day processes and decision-making and integral to the agency management culture. Key risk indicators, key performance indicators, and advanced measurement of risk appetite elements are used to help manage the agency to effectively and efficiently achieve its mission.

06 *Embed fraud risk management in ERM.*

As discussed earlier, Green Book principle 8 – "*Management should consider the potential for fraud when identifying, analyzing, and responding to risks*" – signifies the intersection of fraud risk management in ERM. Principle 8 and GAO's Fraud Risk Management Framework are highlighted and prescribed in the revised Circular A-123, and the GAO Framework is the cornerstone of the Fraud Reduction and Data Analytics Act of 2015. As shown in Appendix 2 of this white paper, GAO's Framework[45] organizes leading practices encompassing activities to prevent, detect, and respond to government fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks in federal programs. The GAO Framework also highlights the importance of monitoring and incorporating feedback.

While OMB Circular A-123 and the GAO Framework largely address fraud risks in the context of principle 8, fraud risk management occurs throughout all five components of the Green Book. For example, part of establishing the control environment is considering how fraud risk management could impact the organizational structure. Where the significance of fraud risk to achieving the entity's objectives is high, establishing an antifraud unit to manage this risk may be advisable. The Green Book expects this type of consideration by management.

IGs will continue to play an important role in assessing fraud risks, detecting and investigating fraud, and making recommendations to management on corrective actions to address identified fraud risks. They are clearly an important part of an agency's ERM team. At the same time, the Green Book makes clear that agency management and staff must be actively engaged as the first line of fraud defense. An essential element is management's day-to-day monitoring and evaluation to ensure control activities are operating as intended and timely action is taken to mitigate any identified breakdowns and weaknesses.

07 *Identify risks and mitigation actions.*

In moving to OMB's ERM and fraud risk management mandate in Circular A-123 and the requirements of the Fraud Reduction and Data Analytics Act of 2015, agencies will not be starting with a clean sheet of paper. Since 1982, the FMFIA process has been a means of identifying risks to mission achievement, accountability, and asset safeguarding. Included are major risks that transcend an agency or even several agencies, such as cybersecurity, contract and grant management, and improper payments. Fully leverage this process, with a much broader eye to connecting the dots.

Both internal and external factors, as well as inherent risks impacting the agency risk profile must be part of the risk equation. Some risks may be difficult to tackle or outside an agency's direct control, but they must be addressed in line with the agency risk appetite. The risk profile should be a living document, and as mentioned earlier, the result of fact-based analysis and open and candid conversations at every level of the organization.

Circular A-123 recognizes that agencies will generally need to first build their risk management capabilities; followed by implementing ERM techniques to rate risks in terms of mission impact and likelihood; and finally continuously monitor and assess risk developments. Agencies have completed the circle when they have fully incorporated risk awareness into their culture and day-to-day ways of doing business. While recognizing that many approaches are available to implement ERM, using the United Kingdom's Orange Book as a basis, OMB Circular A-123 addressed that at the outset most approaches include elements such as:

- **Establish the context** by understanding and articulating the organization's internal and external environment and risk objectives, which in Circular A-123 are categorized as strategic, operations, reporting, and compliance.

45. See http://www.gao.gov/assets/680/671664.pdf.

- **Initial risk identification** using structured, systematic approaches to identify where there is a potential for undesired outcomes. These represent inherent risks.
- **Assess the adequacy of the response to inherent risks** considering the adequacy of mitigation efforts, such as management controls to reduce risks, and other factors to determine the residual risk.
- **Analyze and evaluate risk** considering the causes, sources, risk probability, and potential outcomes (both positive and negative) as tools to help prioritize residual risks.
- **Develop alternatives** systematically identifying and considering available options, guided by the risk appetite. The risk response is targeted at mitigating residual risk to an acceptable level consistent with the risk appetite. In considering alternatives, organizations should not be encumbered by simply improving upon the status quo and should leverage leading practices and technology enablers.

The ERM Playbook includes guidance and tools. Agencies have flexibility. Among leading practices are risk rating and ranking considering the impact and likelihood of occurrence and the development of risk heat maps.

Tools, such as table-top exercises to test hypotheses and model alternatives to the status quo, can be helpful.[46] The organization would be simulating what could happen. For example, in the world of cybersecurity risk, agencies and their auditors perform penetration testing to assess whether vulnerabilities exist and whether the processes and procedures are properly designed and operating as expected.[47]

Once there is agreement on the residual risks and the mitigation priorities, leading organizations then focus on mitigation or remediation strategies. This is further discussed in critical element 9 and covered in three additional Orange Book elements – respond to risks, monitor and review, and continuous risk identification. In doing so, leading organizations will first focus on the existing processes and procedures and how they are structured and work together across the enterprise. The goal is having a control structure where the whole is stronger than the sum of the parts.

Remember to right-size controls at the same time to focus on what is important. Too much focus in areas having low impact and low likelihood of occurrence can just add bureaucracy, increase cost, and stifle attention to what is important. This is why establishing the risk appetite is such an important component of ERM. Otherwise, everything can become important. In doing so, agencies need to:

- Reinforce the reality that management infrastructure—people and systems—will continue to be stressed given serious fiscal sustainability challenges.[48, 49]
- Use the risk appetite as the criteria to look for areas that may have too many processes and procedures, but perhaps not the right ones.
- Make simplification and efficiency strategic agency goals.
- Challenge the 'one size does not fit all' adage all too often used to justify different systems and processes, where one system or process would get the job done.
- Eliminate one-off systems developed in an era of stove-piped organizations.
- Make standardization and shared services a priority.
- Leverage technology enablers.

08 *Understand the nature and potential impact of long-tail and emerging risks.*

ERM must be both current and future focused. Do not fall into the trap of simply focusing on the current risk environment or isolating risk to your organization. Be fully cognizant of the environment around you. Expect continual changes and anticipate the inevitability of new risks. There is a need to consider both long-tail and emerging risks.

46. For an example of a table-top exercise in the environment of audit readiness in the Department of Defense, see "Practice Makes Perfect: Using 'Table-Top Exercises to Simulate the Audit and Help Achieve Audit Readiness for Personnel Payroll Costs," KPMG Government Institute, May 2012 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2012/dod-audit-readiness-concept-paper.pdf).
47. For example, Federal Information System Controls Audit Manual (FISCAM), issued by GAO, presents a methodology for auditing information system controls in federal and other governmental entities in accordance with professional standards (http://gao.gov/products/GAO-09-232G).
48. See http://www.gao.gov/fiscal_outlook/federal_fiscal_outlook/overview#t=0.
49. "Establishing Long-Term Fiscal Sustainability: Daunting Choices and Shared Sacrifice," by William R. Phillips and Jeffrey C. Steinhoff, AGA *Journal*, fall 2012 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2012/aga-journal-sustainability.pdf).

Long-tail risk refers to risks with a very low likelihood of occurrence, but with potentially devastating impacts. An example is the 2008 mortgage lending meltdown that sparked a financial crisis. ERM forces organizations to take a much more rigorous approach to identifying the existence and likelihood of such a risk. With a long-tail risk, an organization cannot stop at just looking at the likelihood and impact. It must continually look at how the risk is changing over time. Is it increasing, decreasing, or somewhat stable? Has the environment changed? This matters because an organization's response would be different depending on the scenario.

One reason the mortgage lending meltdown emerged is because mortgages had traditionally been low risk, with low default rates and rising housing values. Home mortgages were deemed a safe bet by individuals and organizations investing in mortgage-backed securities, and home buyers, who saw their home values rising. But changes in the industry dramatically changed the risk profile. Mortgages had gone from being an originate-to-hold model, where a bank made the loan and collected payments over its life, to an originate-to-sell model, where the risk of default was transferred to the market place. This risk, which had a long tail, was not recognized until it was too late, with devastating global impacts.

The notion of **emerging risks** can be difficult as well because they may not yet have manifested themselves in ways that the impact is viewed as serious. A key to understanding emerging risks is recognizing that organizations and the environment they operate in are never static. ERM is not a one-time event, but rather a continuous process requiring continual vigilance. The military speaks about situational awareness.

Change brings tremendous opportunity, but also introduces new risks such as with the technology explosion. As highlighted earlier, government and private sector organizations have experienced major, highly publicized data breaches. They may have understood the risks in general terms, but did they understand the continual nature of change associated with those risks as cyber vulnerabilities took on new forms? Since cybersecurity may not have been their core mission, did they view the ultimate responsibility for cyber protection as someone else's job? Did they understand across the enterprise potentially devastating impact to their mission and reputation?

09 *Make risk mitigation a critical component of management expectations.*

As discussed in critical element 7, once the organization has determined there is an enterprise risk, it must then identify and analyze alternatives to mitigate or remediate to an acceptable level consistent with the risk appetite. It bears repeating that mitigation can involve risk acceptance, avoidance, reduction, and/or sharing.

An agency's goal should be to determine the best course of action in its situation considering the full range of alternatives. This will require the identification and weighing of costs and benefits of various options. At the heart of mitigation is first identifying the root cause of the risk and any related vulnerability.

Leading organizations strive for fact-based determinations. The goal is not to just add a Band-Aid when surgical tape is needed, which all too often may have been the case in the past and one reason for the current proliferation of cumbersome management systems. Rather, an agency wants to select the strategy that cost effectively and efficiently mitigates the risk to an acceptable level consistent with the risk appetite.

This typically requires a higher degree of sophistication as trade-off decisions can be complex and may require analysis of underlying data to develop actionable mitigation plans. Making better choices through ERM should be a strategic goal. There is a training and staff recruitment component to this building block as federal agencies may need to recruit additional staff with high-end analytic skills, retrain existing personnel, or both.

Mitigation plans should:

Identify 'the' root cause: It is absolutely imperative to identify and understand the root cause of risks; otherwise, organizations can end up treating the symptoms of a problem. Do not stop looking when you identify a cause. The root cause may transcend multiple organizations within an agency, multiple agency programs and operations, multiple agencies, multiple levels of government, and/or the private sector. It may be a byproduct of the organization's culture, or a multitude of other reasons such as legislation and disruptive technology. Guard against making too quick a judgment as to the root cause, or considering risks individually

without the context of the enterprise. Make sure you are fixing the right problem and not inadvertently introducing new risks.

Define expectations: Top management should reinforce its commitment to sound ERM principles. Again, it wants everyone to understand the situation and own the solutions. Organizations will generally need to step outside their comfort zone to move beyond the status quo. This is an element of cultural transformation that will need to become part of the fiber of an organization. Addressing an enterprise risk can be difficult. It generally is not about change at the margin. Reflecting back to the housing meltdown, the subsequent changes in the financial industry have been significant.

Establish action steps: Define strategic and tactical actions to mitigate the risk in line with the risk appetite. Working in partnership across organizations and management silos can be a critical component in establishing the root cause and targeting solutions. Included should be the adoption or expansion of data and technology enablers, such as powerful analytic tools to help prevent improper payments.[50]

Leverage leading practices: There can be a natural tendency to feel your organization is unique and requires tailored solutions to its enterprise risks when the wheel has already been invented by someone else. Look for leading practices, including standardization, moving to shared services, or outsourcing for those activities that are not core agency missions.

Be honest about resource needs: While it can be, do not expect risk mitigation to be resource neutral in the short term. Determine resource needs and match them to existing staff capabilities and financial resources. Over time, addressing an enterprise risk can result in reduced cost and/or increased program and service delivery outcomes that far outweigh the investment. By taking an enterprise view, top management can consider available resources across the agency and the benefits to be derived, both quantitative and qualitative and both short and long term.

Set a deadline: Mitigation requires timely action, for which strong commitment of top management must be a priority. While time lines should be realistic, they should also be in line with the magnitude of the risk presented. For instance, 6 of the 32 items currently on GAO's High-Risk List have been on the list for over 25 years, and another 14 have been on the list for at least 10 years.[51] In contrast, following President Kennedy's historic May 1961 challenge[52] to put a man on the moon, it took the United States 8 years to accomplish the mission.[53]

Assign a "hammer": Someone has to be on point to drive the nail as needed and ensure things get done. Responsibility and accountability must be accompanied by top management support, an ability to act across the enterprise, the requisite authority to make decisions within certain predetermined parameters, and a commitment for support as needed across agency organizations and among stakeholders. Without these conditions, responsibility and accountability are difficult to enforce, which can be a reason that actions to address known risks have continued to languish or in the end do not address the root cause.

10 *View this as a never-ending marathon and not a sprint, and get started!*

Lessons learned during the early years of FMFIA implementation provide valuable insights. Don't try to boil the ocean by establishing massive assessment and reporting programs on day one. Guard against the process becoming the measurement of success. Yes, as described in the earlier nine critical elements, governance and the other implementation steps provide a disciplined process, but the measure of success is whether the agency is effectively and efficiently managing its risks within its risk appetite and adding value through ERM. Instead, adopt incremental steps, focusing initially on a relatively small number of top risks. Then build from the initial foundation.

This does not mean start slowly, but start smartly with clear purpose. Leading organizations work to embed ERM into business processes as a normal 'way of doing business.' This represents transformational change that will take time and perseverance. Leading organizations

50. "Calling All Government Financial Managers to a More Analytic Role," by David A. Fitz, James P. Hauer III, and Jeffrey C. Steinhoff, AGA *Journal*, summer 2015 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2015/aga-data-analytics.pdf). For example, since 2008, the Department of Defense as prevented billions of dollars of improper payments through use of data analytic tools (https://paymentaccuracy.gov/content/success-stories).
51. "HIGH RISK SERIES: An Update," GAO-15-290, February 11, 2015 (http://www.gao.gov/assets/670/668415.pdf).
52. See http://history.nasa.gov/moondec.html.
53. See http://www.nasa.gov/mission_pages/apollo/apollo11.html.

have the patience and discipline to find the appropriate balance between the short- and long-term needs of the organization and to build the foundation for continual success.

Getting started can be especially challenging in large organizations, which are widely disbursed and have a multitude of missions, strategic objectives, programs, operations, and stakeholders. Learning to walk before running becomes important. Build the ERM initiative incrementally, focusing first on those areas known to be the highest risk. Widely share early successes in the organization to encourage others by demonstrating what can be achieved. Agencies want both early successes and early lessons learned as to what works well and what does not in implementing transformative change impacting the entire organization. This is not to say it should take years to move forward, but it should be deliberative and well planned and executed. Mark Twain said it well: "*The secret to getting ahead is getting started. The secret of getting started is breaking your complex overwhelming tasks into small manageable tasks, and then starting on the first one.*"[54]

In getting started, view laws, rules, regulations, and standards as the floor. Leading organizations go beyond minimal compliance with Circular A-123 and the Green Book. They view requirements and standards from OMB and GAO as a framework of tools to help them carry out their mission in the public interest, with full accountability and transparency. They know that simply demanding compliance and nothing more can frustrate meaningful results, impair innovation, and lead to a check-the-box exercise with minimal value.

Adding value

The 10 critical elements are intended to work together, with a focus on results and not on establishing a record of compliance with Circular A-123 and the Green Book. In moving to ERM, it is critical to avoid the pitfalls initially experienced under FMFIA, whereby assessment and reporting processes quickly became the end game and grew into massive paperwork exercises.[55] To quote from 2005 GAO testimony[56] before the Subcommittee on Government Management, Finance, and Accountability[57] of the House Committee on Government Reform,[58] reflecting on the fact there was too much process and paper associated with FMFIA implementation:

"…. *what started off as a well-intended program to foster continual assessment and improvement of internal control unfortunately had become mired in extensive process and paperwork. Significant attention was placed on creating a paper trail to prove that agencies had adhered to the OMB assessment process and on crafting voluminous annual reports that could exceed several hundred pages. It seemed that the assessment and reporting processes had, at least to some, become the endgame.*[59]

At the same time, there were some important accomplishments coming from FMFIA. Thousands of problems were identified and fixed along the way, especially at the lower levels where internal control assessments were performed and managers could take focused actions to fix relatively simple problems. Unfortunately, many of the more serious and complex internal control and accounting weaknesses remained unchanged and agencies were drowning in paper."

It will be important to ***demonstrate value*** through results that otherwise may not have been reasonably possible without an ERM program. If implementation of the changes to Circular A-123 and the Green Book become compliance exercises, agencies may end up introducing a new risk by diverting resources to processes of questionable value versus other more valuable alternatives for risk management.

Proactively manage risk to protect against surprises, stabilize performance, and operate within the agency's risk appetite. Look for opportunities to improve performance through decision-making that considers the agency's risk profile and understands the cost and benefit of mitigation alternatives as a means of improving resource allocation and safeguarding assets. Finally, leverage data and technology to provide risk intelligence and establish an appropriate risk culture across the agency that focuses on risk beyond organizational stovepipes.

---

54. See http://thinkexist.com/quotation/the_secret_of_getting_ahead_is_getting_started/216812.html.
55. "Financial Integrity Act: Inadequate Controls Result in Ineffective Federal Programs and Billions of Dollars in Losses, GAO/AFMD-90-10, November 28, 1989 (http://www.gao.gov/assets/150/148414.pdf).
56. "FINANCIAL MANAGEMENT – Effective Internal Control is Key to Accountability," Statement of Jeffrey C. Steinhoff, Managing Director, Financial Management and Assurance, GAO-05-321T, February 16, 2005 (http://www.gao.gov/assets/120/111338.pdf).
57. The Subcommittee has since been renamed the Subcommittee on Government Operations.
58. The Committee has since been renamed the Committee on Oversight and Government Reform.
59. The "OMB assessment process" is the process established under Circular A-123.

Appendix 1
The 17 Internal Control Principles

Control Environment

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.

2. The oversight body should oversee the entity's internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Risk Assessment

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Source GAO. I GA0.14.704G

Control Activities

10. Management should design control activities to achieve objectives and respond to risks.

11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

12. Management should implement control activities through policies

Information and Communication

13. Management should use quality information to achieve the entity's objectives.

14. Management should internally communicate the necessary quality information to achieve the entity's objectives.

15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

Monitoring

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

17. Management should remediate identified internal control deficiencies on a timely basis.

Appendix 2
GAO's Fraud Risk Management Framework

Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.

— Demonstrate a senior-level commitment to combat fraud and involve all levels of the program in setting an antifraud tone.

— Designate an entity within the program office to lead fraud risk management activities.

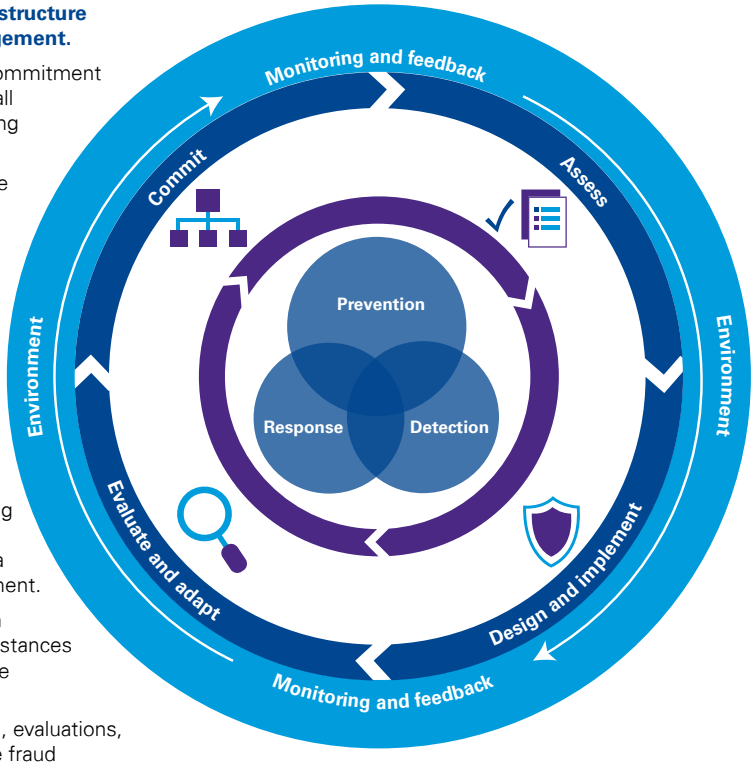
— Ensure the entity has defined responsibilities and the necessary authority to serve its role.

Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.

— Conduct risk-based monitoring and evaluation of fraud risk management activities with a focus on outcome measurement.

— Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends.

— Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.



Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

— Tailor the fraud risk assessment to the program. and involve relevant stakeholders.

— Assess the likelihood and impact of fraud risks and determine risk tolerance.

— Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.

Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.

— Develop, document, and communicate an antifraud strategy, focusing on preventive control activities.

— Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.

— Establish collaborative relationships with stakeholders, and create incentives to help ensure effective implementation of the antifraud strategy.

Source GAG | GAD – 15-5035P

The GAO Framework also includes valuable insights in a series of appendices covering:

— Challenges related to measuring fraud

— Examples of control activities and additional information on leading practices for data analytics and fraud-awareness initiatives

— Risk factors for assessing improper-payment risk

— Example of a fraud risk profile

See http://www.gao.gov/assets/680/671664.pdf.

Appendix 3

OMB Circular A-11 guidance on the role of a federal CRO

"…. *An effective enterprise risk manager does the following:*

- *Develops, manages, coordinates, and oversees a comprehensive system for proactively, identifying, prioritizing, monitoring, and communicating an organization's enterprise-wide risks. Such risks include relevant strategic, operational, financial, and programmatic barriers as well as reputational risks that could interfere with an organizations defined strategic objectives or performance goals.*
- *Oversees the development and use of a robust set of risk management indicators that are representative of organizational operations and prioritized risks.*
- *Establishes and provides oversight of policies that enable consistent use of enterprise risk management principles and supports an integrated view of risk across the organization.*
- *Ensures the incorporation and dissemination of enterprise-wide risk management protocols and best practices is appropriate for the whole organization to reduce duplication of effort and improve agency performance.*
- *Establishes the procedures for determining the amount of risk an agency will accept or mitigate, including the manner in which these elements of decision-making are documented.*
- *Creates and maintains institutional capacity and accountability for risk management through the exchange of information, knowledge, education and training staff."*

See OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget,* sections 270.24 to 270.28, July 2015 (https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a11_2016.pdf).

Appendix 4

Questions related to establishing the risk appetite and additional context

1. What do we lose sleep over?
2. What do we not want to see on the news or in blogs?
3. What are the expectations of stakeholders, such as the public, the President, and the Congress?
4. What do we want to make sure happens and happens well? (Risk management is not simply about avoiding problems, but encompass facilitating results envisioned in the agency strategic plan and expected by stakeholders.)
5. What problems have occurred or are emerging in other organizations that could be a problem in our agency as well? (This requires organizations to share information and establish ongoing channels of communication to keep their finger on the pulse of what is happening more broadly in the world that may impact their risks.)
6. Have changes in the agency or external to the agency introduced new or expanded risks?
7. What risks are looming on the horizon?
8. Which risks may have a long tail?
9. What policies and procedures are now in place to mitigate risks? How are they working? What about their cost and benefits? (Not knowing this information could in itself represent an organizational monitoring and oversight risk.)
10. What level of risk mitigation can we reasonably afford? How do we get the most 'bang for the buck' assuming resources fall short of needs? (The cost of not focusing on the right risks at the right time in the right way may exceed the cost of taking mitigation actions. So both the current investments and longer-term costs and benefits must be part of the equation.)

Acronyms

AGA: Association of Government Accountants

CFO: Chief Financial Officer

CFO Act: Chief Financial Officers Act of 1990

Circular A-11: OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*

Circular A-123: OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*

COSO: Council of the Sponsoring Organizations of the Treadway Commission

CRO: Chief risk officer

ERM: Enterprise risk management

FMFIA: Federal Managers' Financial Integrity Act of 1982

GAO: U.S. Government Accountability Office

GAO Framework: *A Framework for Managing Fraud Risks in Federal Programs*

GPRA: Government Performance and Results Act of 1993

GPRMA: Government Performance and Results Modernization Act of 2010

Green Book: Comptroller General's *Standards for Internal Control in the Federal Government*

IG: Inspector General

NBES: National Business Ethics Survey

OMB: U.S. Office of Management and Budget

Orange Book: United Kingdom's *Management of Risk – Principles and Concepts*

SEC: U.S. Securities and Exchange Commission

RMC: Risk management council

Related KPMG thought leadership

Enterprise risk management: Protecting and enhancing value, KPMG LLP, September 2016

Ten Steps to Sustainable Enterprise Risk Management, *Journal of Government Financial Management*, Summer 2016, AGA, by Laura A. Price, Jeffrey C. Steinhoff, Timothy J. Comello, and Thomas A. Cocozza, KPMG LLP

Pushing the envelope on competitive advantage – Developing your risk management function for the future, KPMG (China), 2016

Vision, strategy & structure – Optimizing Governance, Risk and Compliance Programs, KPMG LLP, February 2016

Key risk management issues for 2016 – Risk issues and opportunities that should top chief risk officers' agendas, KPMG LLP, February 2016

Calling All Government Financial Managers to a More Analytic Role as Highly-Valued Business Advisors!, Journal of Government Financial Management, Summer 2015, AGA, by David A. Fitz, James P. Hauer, and Jeffrey C. Steinhoff, KPMG LLP

High-Performing State Medicaid Integrity Programs: Putting It All Together in the "Final Mile," KPMG Government Institute, November 2014

Are You Combat Ready to Win the War Against Improper Payments?, *Journal of Government Financial Management*, Summer 2014, AGA, by Danny Werfel, Boston Consulting Group, and Jeffrey C. Steinhoff, KPMG LLP

Expectations of Risk Management Outpacing Capabilities – It's Time For Action, KPMG International, May 2013

Smart Use of Data Mining is Good Business and Good Government, *Journal of Government Financial Management*, Spring 2012, AGA, by Jeffrey C. Steinhoff and Terry L. Carnahan, KPMG LLP

Don't Delay – The Time Has Come to Use the Full Potential of Enterprise Risk Management to Reduce Costs and Enhance Program Delivery, *Journal of Government Financial Management*, Winter 2011, AGA, by Jeffrey C. Steinhoff and Geoffrey L. Weber, KPMG LLP

Falsifying Government Claims and Insider Trading – Feds are Vigilant in Wake of Economic Crisis, ACFE *Fraud* Magazine, November/December 2011, by Richard H. Girgenti, J.D., CFE, KPMG LLP

Managing the Risk of Fraud and Misconduct: Meeting the Challenges of a Global, Regulated, and Digital Environment, by Richard H. Girgenti, J.D., CFE, and Timothy P. Hedley, Ph.D., KPMG LLP (New York: The McGraw-Hill Companies, Inc., 2011)

Turning risk into advantage – KPMG's Evolving World of Risk Management, KPMG LLP, 2011

Risk Management – A Driver of Enterprise Value in the Emerging Environment, KPMG LLP, 2011

A Practical Look at How Government Agencies Can Reduce Improper Payments, KPMG Government Institute, March 2011

Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance, KPMG LLP

Understanding and articulating risk appetite, KPMG LLP, 2009

The KPMG Executive Guide to High Performance in Federal Financial Management, KPMG Government Institute, June 2009

Forensic Auditing – A Window to Identifying and Combating Fraud, Waste and Abuse, *Journal of Government Financial Management*, Summer 2008, AGA, and AGA Weblog, June 23, 2008, by Jeffrey C. Steinhoff, KPMG LLP

Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response, KPMG LLP, 2006

How KPMG can help

Developing a sustainable, value-added ERM program is an art. For over a century, KPMG has worked with federal agencies to help them achieve the highest level of integrity across their most important and complex programs and operations. KPMG has deep experience facilitating and guiding large, complex organizations through the ERM journey from design to implementation to report.

We offer unique context, with members of our team having served in leadership positions in the federal government, such as working with the Congress on passage of FMFIA and leading GAO's development of the Green Book and oversight of FMFIA implementation. We offer an approach to risk management with capabilities and methodologies to identify and seize opportunities, to understand the impact of risk on mission performance, and to use that knowledge to help you make changes across people, processes, functions, and layers of the organization to mitigate strategic, operational, and external risks.

Our in-depth understanding of government programs, regulatory experience, financial and program audit capabilities, forensic technology, and fraud risk management services enable us to help our clients develop, implement, and manage thorough risk management programs.

Our extensive methodologies and tools address the following ERM framework elements and can be tailored to agency needs:

Acknowledgements and contacts

This white paper was developed by the KPMG Government Institute under the leadership of Managing Director, Jeffrey C. Steinhoff, and with the support of Christopher R. Marston, principal in charge, Federal Advisory, and Diane L. Dudley, partner in charge, Federal Audit.

Contact us

To learn more about leading practices for ERM and fraud risk management, please contact us.

Laura A. Price
Partner, Risk Consulting Leader
Federal Advisory
T: 703-286-8460
E: lprice@kpmg.com

David B. Buckley
Managing Director,
Fraud Risk Management, Federal Advisory
T: 703-286-8489
E: davidbuckley@kpmg.com

Thomas A. Cocozza
Director, Risk Consulting
Federal Advisory
T: 703-286-6835
E: tcocozza@kpmg.com

Timothy J. Comello
Managing Director, Risk Consulting
Federal Advisory
T: 703-286-8580
E: tcomello@kpmg.com

Edmund L. Green
Managing Director, Risk Consulting, and Member of KPMG's National ERM Leadership Team
T: 703-286-8692
E: elgreen@kpmg.com

Visit the KPMG Government Institute at:

www.kpmg.com/us/governmentinstitute

Jeffrey C. Steinhoff
Managing Director, KPMG Government Institute
T: 703-286-8710
E: jsteinhoff@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.