Ten Steps to Sustainable Enterprise Risk Management

Copyright 2016. Association of Government Accountants. Reprinted with permission. All rights reserved.

By: Jeffrey C. Steinhoff, CGFM, CPA, CFE, CGMA; Laura A. Price, MA, CGFM, CPA; Timothy J. Comello, CPA; and Thomas A. Cocozza, MBA, CGFM, CPA

Whether in professional or personal lives, we all face continuing uncertainty or risk. Successfully navigating uncertainty to our advantage is what counts. Risk management can be as complex as keeping fraud perpetrators out of multi-billion-dollar emergency relief programs, or as simple as knowing which route to take to avoid gridlock and make it to your child's class play on time. In both cases, there are uncertainty, risk of failure and options to consider.

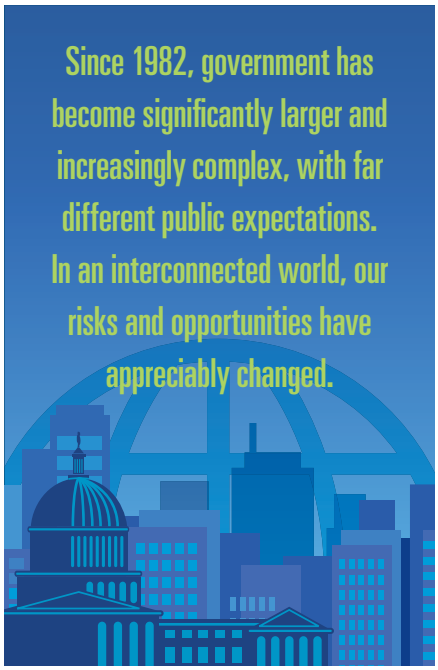
Expectations for addressing the risk of fraud, waste, abuse and mismanagement increased dramatically in 1982 with enactment of the Federal Managers' Financial Integrity Act (FMFIA).[1] Three decades later, there's another dramatic turn through pending new requirements for enterprise risk management (ERM) by the Office of Management and Budget (OMB).

This article explores how the internal control compass of our profession can help government managers better navigate uncertainty through ERM concepts that have been battle-tested for decades. We focus on key issues surrounding the why and how of what will be transformative change by highlighting 10 critical implementation elements.

CHANGING DIRECTION

FMFIA changed the direction of internal control from focusing primarily on accounting and financial reporting controls to broader consideration of program and operation controls, or management control. FMFIA addresses the entire range of policies and procedures that management employs to perform its mission efficiently and effectively, and to provide full accountability to the taxpayer. It covers programs, activities, operations and functions.[2] FMFIA reinforces that internal controls are an integral part of achieving agency mission goals and objectives, providing reliable day-to-day and annual financial reporting, and supporting compliance with laws and regulations, both program and financial.

Agency management is required to assess and report annually on the adequacy of internal controls to meet FMFIA's objectives. Pursuant to FMFIA, *Standards for Internal Control in the Federal Government* (Green Book) were issued by the Government Accountability Office (GAO).[3] Also, FMFIA assessment and reporting guidance are contained in OMB Circular A-123.



Since 1982, government has become significantly larger and increasingly complex, with far different public expectations. In an interconnected world, our risks and opportunities have appreciably changed. Data has become an asset to be protected like currency or gold,[4] and analytic tools are game-changers.[5] The public expects much greater program integrity, and transparency into operations, spending and performance. Finally, while FMFIA has provided continuing focus on internal controls, major control breakdowns continue to emerge, demonstrating the need to rethink the approach. Battle-tested for decades, the movement to ERM has begun.

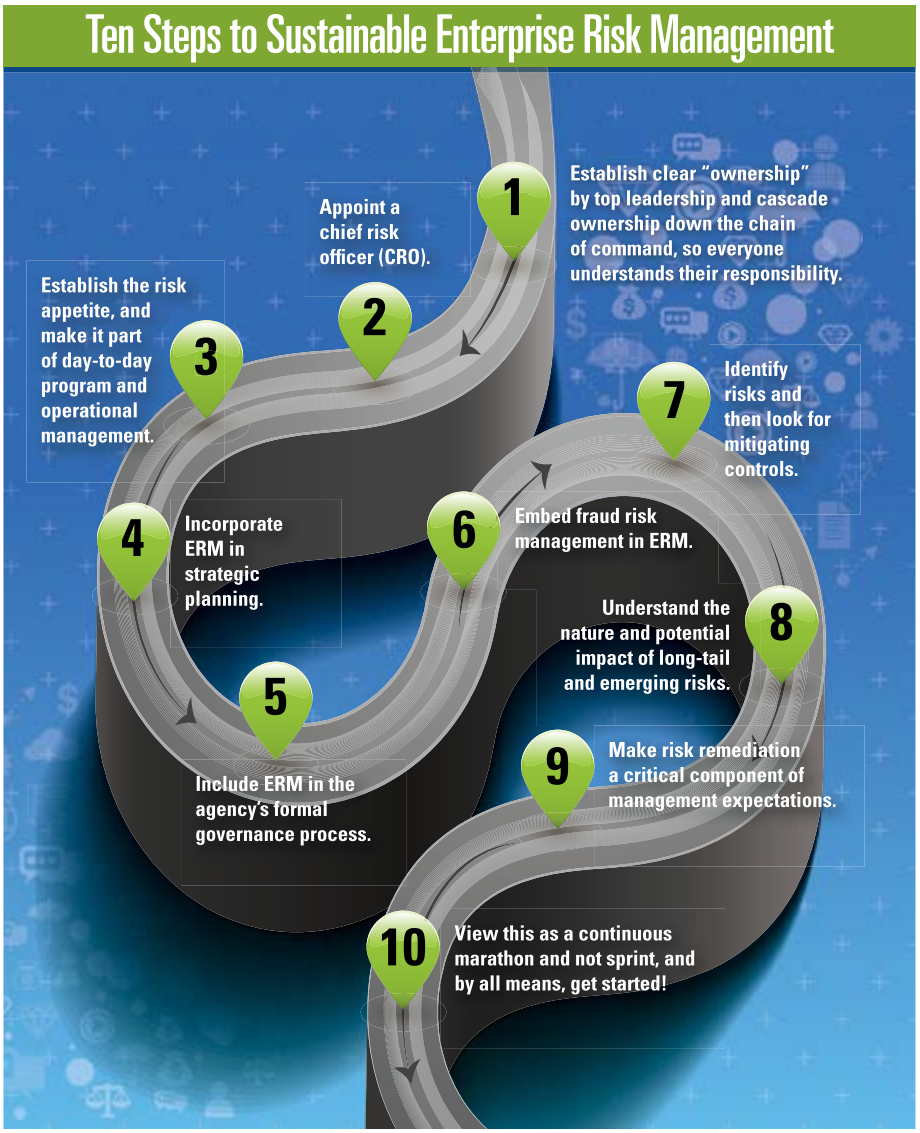
In its 2004 *Enterprise Risk Management — Integrated Framework*, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[6] said it well: "Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to more effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value."[7]

In a 2013 update of its *Internal Control — Integrated Framework*,[8] which the Green Book first adapted to the government environment in 1999, COSO introduced 17 principles related to the five internal control components.[9] A major update to the 2014 Green Book, issued in September 2014, incorporates these principles and includes additional information on internal control attributes.

The most significant revision to Circular A-123 in 30 years is intended to modernize FMFIA efforts by

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 583305

Copyright 2016. Association of Government Accountants. Reprinted with permission. All rights reserved.



integrating risk management and internal control activities into ERM. The objective is to improve mission delivery, reduce costs, and focus corrective actions toward key risks. As OMB has emphasized, ERM:[10]

> "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."

MOVING TO THE NEXT STAGE

Successful evolution to ERM requires transformative thinking and partnerships between program and operational leadership, including chief risk officers (CROs), chief financial officers (CFOs), and inspectors general (IGs). These leaders must collaboratively break down barriers and organizational silos inhibiting consideration of enterprise risks across agency components and between agencies. From the Institute of Management Accountants: ERM "is a truly holistic, integrated, forward-looking, and process-oriented approach to managing all key business risks and opportunities — not just financial ones."[11]

You're probably thinking, "easier said than done," since ERM represents cultural transformation and not a technical challenge. We agree. This won't happen unless leaders see ERM as a means to help:

- achieve a government that costs less and works better, by delivering public services in a manner that rebuilds public confidence;
- align scarce resources by starting first with the highest risks to program delivery and operational breakdowns, fraud, waste, abuse and mismanagement;
- better balance risks, rewards, costs and benefits in line with a defined risk appetite, tied to agency missions and strategic goals; and
- leverage data through enabling technology to provide risk intelligence and establish a risk culture that looks beyond organizational stovepipes.

CRITICAL ELEMENTS

Incorporating ERM into day-to-day operations requires transformation through top management leadership and disciplined approaches — common denominators in leading organizations. We offer 10 critical elements to consider for a sustainable ERM implementation strategy that can add value to program and operational managers in effectively and efficiently accomplishing missions and strategic goals.[12]

1 Establish clear "ownership" by top leadership and cascade ownership down the chain of command, so everyone understands their responsibility.

Planned 2016 changes to Circular A-123 and the changes in the 2014 Green Book are transformative, with success largely hinging on changing the organization's management culture. There must be a sense of urgency, clear expectations, recognition for success, and accountability for failure. This starts at the top, and clear direction and a sense of urgency are imperative.

2 Appoint a CRO. This individual should be adequately empowered, and have sufficient capabilities and

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 583305

Copyright 2016. Association of Government Accountants. Reprinted with permission. All rights reserved.

resources to add value in supporting program and operational management. Top leadership must establish the right relationship for the CRO throughout the agency, with an understanding by program and operational management that ERM is ultimately their responsibility. The CRO should be supported by the CFO and IG, who can add valuable insights and practical experience.

3 Establish the risk appetite, and make it part of day-to-day program and operational management. Risk appetite is the heart of ERM, and reflects the mission and strategy, including organizational objectives, strategic plans and stakeholder expectations. Management acknowledges a willingness and capacity to take some level of risk, and has a tolerance for some level of loss or other negative results. There's recognition that attempting to set up costly, fail-safe systems to avoid all risk is unrealistic or unnecessary, and being overly cautious can carry too high a price. The risk appetite is intended to help drive decisions based on relative priorities and the balance between control and cost.[13] Leading organizations carefully define the risk appetite and communicate what it means across the entity. They develop a common understanding of what, who, when, and why. They engage stakeholders, including legislators and the public, so there's shared understanding and no surprises.

4 Incorporate ERM in strategic planning. Strategic plans reinforce top management's priorities and expectations. Strategic planning provides an opportunity to identify and break down organizational barriers impeding effective and efficient ERM implementation. Eliminating organizational stovepipes and promoting enterprise partnerships between programs and operations are essential components to affecting meaningful change and establishing value. Again, as discussed in critical element 1, this starts with top management and must be a high enough priority to resonate with program and operational leadership, who may view ERM and fraud risk management the responsibility of the CRO, CFO, and/or IG, or who simply may not care.

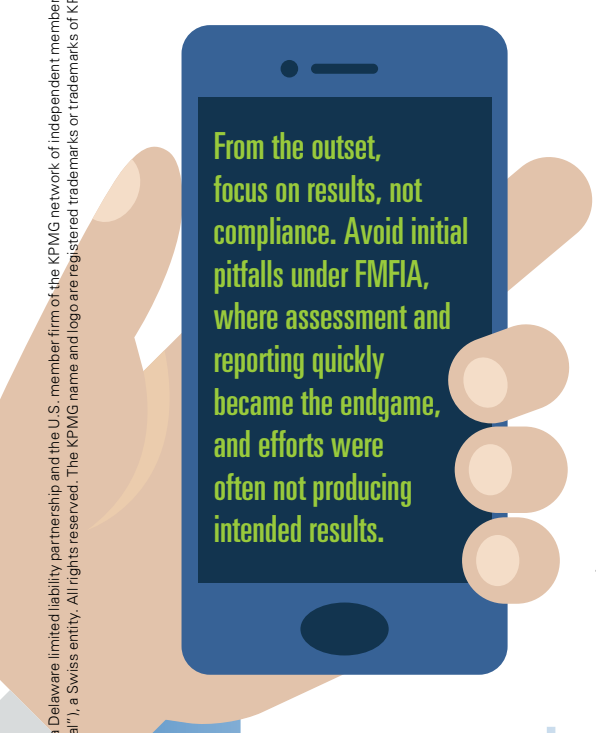
5 Include ERM in the agency's formal governance process. View ERM as a component of governance, supported by internal control and fraud risk management. ERM governance should include:

- Clear roles and responsibilities linking to all 10 critical elements.
- Well-designed policies and procedures covering risk assessment, identification, categorization and remediation.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 583305

Copyright 2016. Association of Government Accountants. Reprinted with permission. All rights reserved.

- Fact-based trade-offs between control and cost, alternatives, and the relative importance of risks associated with different programs and operations.[14] Leading organizations want to select the right controls, while eliminating controls that no longer add sufficient value. This requires a high degree of sophistication, since trade-off decisions can be complex and require extensive data gathering and analysis.
- Documentation of key judgments in a manner that avoids excessive process and paperwork that plagued the early years of FMFIA implementation.[15] COSO said it well in its 2013 Integrated Framework: "Management would need to document significant judgments."
- Oversight and monitoring driven by meaningful and reliable metrics to gauge performance and risk impacts.
- Education focused on content and context and provided agency-wide.



- Open communication to raise risks and share lessons learned without fear of retaliation or negative career repercussions.
- Incentives for people to do the right thing, transparency to help assure they do and effective accountability mechanisms if they don't.
- Continuous reevaluation of the risk environment, so it becomes embedded in the management fiber driving day-to-day decision-making.
- Stakeholder involvement and partnership, including business partners in other agencies and levels of government.
- Coordination with the IG to share intelligence on risks and leading practices. Under *Government Auditing Standards*,[16] whereas auditors cannot make agency management decisions or perform management functions, they can provide routine advice and respond to questions, including sharing leading practices.[17]
- Strong working relationships with the CFO, who brings valuable internal control capability and works across the agency.
- Maturity models as tools to define, measure and build ERM program maturity.

6 Embed fraud risk management in ERM. Green Book principle 8 signifies the intersection of fraud risk management and ERM: "Management should consider the potential for fraud when identifying, analyzing, and responding to risks." Complementing principle 8, in July 2015, GAO issued *A Framework for Managing Fraud Risks in Federal Programs* (Framework).[18] The Framework organizes leading practices encompassing control activities to prevent, detect and respond to fraud, with emphasis on prevention. It is expected that the revised Circular A-123, citing principle 8, will require adherence to the Framework's leading practices. IGs will continue to play their important audit and investigation roles when it comes to fraud. At the same time, agency management and staff are still the first line of fraud defense.

7 Identify risks and then look for mitigating controls. Leading organizations first identify risks, followed by control assessments and mitigation priorities. Agencies should fully leverage existing FMFIA processes, and widen the aperture to focus on control structures and how controls work together to help ensure adequate risk mitigation.

Remember to right-size controls to focus on what's important. American philosopher and psychologist William James said, "The art of being wise is knowing what to overlook." Too much control in low-risk, low-impact areas adds bureaucracy and diverts attention from what's important, thereby introducing additional risk. Finding the right balance strengthens control while reducing costs and underlines why establishing the risk appetite is so important.

8 Understand the nature and potential impact of long-tail and emerging risks. Long-tail risks have very low likelihoods, but potentially devastating impacts. Think of the housing meltdown, which sparked the 2008 financial crisis. It was largely overlooked, including by public-employee pension funds that invested in mortgage-backed instruments, long-considered to be rock-solid, low-risk investments.

Emerging risks can be difficult to identify because they have not yet manifested themselves such that they are viewed as serious risks. Key to understanding emerging risks is recognizing that organizations and their environments constantly change. The military calls this situational awareness: always understanding where you are with respect to achieving the mission and what unexpected or new roadblocks stand in the way.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 583305

Copyright 2016. Association of Government Accountants. Reprinted with permission. All rights reserved.

9 Make risk remediation a critical component of management expectations. Most importantly, identify and address the root cause and address problems in a timely manner. Without understanding the root cause, organizations risk treating only the symptom of the problem. The IGs and GAO have thousands of open recommendations. It's an enterprise risk when known problems languish for years or even decades.[19]

Remediation plans should: (1) identify the root-cause, (2) define expectations, (3) establish action steps, (4) leverage leading practices, (5) be honest about resource needs, (6) set a deadline and (7) assign a "hammer" to drive results. Think of data and technology as integral remediation enablers. Increasingly more-powerful analytic tools, including algorithms, can convert mountains of data into business intelligence to help manage risk and prevent and detect fraud, waste and abuse.[20]

10 View this as a continuous marathon and not sprint, and by all means, get started! The process never ends, making it imperative to embed ERM and fraud risk management considerations in routine, day-to-day management. While not a sprint, avoid the temptation to wait for others. Often attributed to Mark Twain: "The secret of getting ahead is getting started."

Likewise, through careful planning, learn to walk before running. Agencies want both early successes and lessons-learned in implementing transformative change impacting the entire organization. Adopt incremental steps, focusing initially on a relatively small number of top risks.[21] Then build from this foundation to eventually embed ERM into daily business processes.

From the outset, focus on results, not compliance. Avoid initial pitfalls under FMFIA, where assessment and reporting quickly became the endgame, and efforts were often not producing intended results.[22] View laws, rules, regulations and standards as baseline requirements. Consider Circular A-123 and the Green Book as tools in executing the mission, and recognize that simply complying with requirements for compliance's sake can frustrate meaningful results, limit innovation and lead to a check-the-box mentality with sub-optimized value.

FINAL THOUGHTS

Public expectations and long-term fiscal sustainability[23] demand bold, transformative action to achieve government that costs less and works better by delivering public services in a manner that rebuilds public confidence. Working collaboratively, program, operational and financial managers can use ERM, including fraud risk management, to target the highest risks to program delivery and operational breakdowns, fraud, waste, abuse and mismanagement.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 583305

Copyright 2016. Association of Government Accountants. Reprinted with permission. All rights reserved.

Seize the opportunity to better balance risks, rewards, costs and benefits in line with a defined risk appetite, tied to the organization's mission and strategic goals. Move to enterprise solutions that connect the dots to help protect against unwelcome surprises, improve decision-making and performance, strengthen resource allocation and asset safeguarding, and reduce costs. Assisted by enabling technology, leverage data to provide risk intelligence. Establish a risk culture that looks beyond organizational stovepipes. Aspire to embed ERM in normal day-to-day decision-making and operations, so it's not viewed as a stand-alone activity and becomes second nature.

The challenge today is to vigorously begin the journey to the next level in meeting the expectations of the Congress and the president when FMFIA was enacted and signed into law in 1982. To borrow the words of Arthur Ashe: "Start where you are. Use what you have. Do what you can."

Endnotes

1. See https://www.whitehouse.gov/omb/financial_fmfia1982
2. "FINANCIAL INTEGRITY ACT: Inadequate Controls Result in Ineffective Federal Programs and Billions in Losses," GAO/AFMD-90-10, November 1989 (http://www.gao.gov/assets/150/148414.pdf).
3. See http://www.gao.gov/assets/670/665712.pdf
4. The 2012 World Economic Forum declared data an economic asset, like currency or gold.
5. "Calling All Government Financial Managers to a More Analytic Role," by David A. Fitz, James P. Hauer III, and Jeffrey C. Steinhoff, Association of Government Accountants (AGA) *Journal of Government Financial Management*, summer 2015 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2015/aga-data-analytics.pdf).
6. See http://www.coso.org/aboutus.htm
7. See http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf
8. See http://www.coso.org/ic.htm
9. The five components are (1) control environment, (2) risk assessment (3) control activities, (4) information and communications, and (5) monitoring.
10. OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, June 2015 (https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s270.pdf).
11. IMA, "Enterprise Risk Management: Frameworks, Elements, and Integration," 2011 (http://www.imanet.org/docs/default-source/research/sma/erm_frameworks-elements-and-integration.pdf?sfvrsn=2).
12. Also see an earlier article in the *Journal of Government Financial Management*, "Don't Delay — The Time Has Come to Use the Full Potential of Enterprise Risk Management to Reduce Costs and Enhance Program Delivery," by Jeffrey C. Steinhoff and Geoffrey L. Weber, *Journal of Government Financial Management*, winter 2011 (https://www.agacgfm.org/AGA/JournalOnline/2011Winter/SteinhoffWeber.pdf).
13. "Understanding and articulating risk appetite," KPMG Australia Advisory, June 2008, (https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Risk-appetite-O-200806.pdf).
14. OMB Memorandum-07-24, *Updated Principles for Risk Analysis*, and OMB Circular A-129, *Policies for Federal Credit Programs and Non-Tax Receivables* (https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-24.pdf and https://www.whitehouse.gov/sites/default/files/omb/assets/a129/rev_2013/pdf/a-129.pdf).
15. "FINANCIAL MANAGEMENT — Effective Internal Control is Key to Accountability," Statement of Jeffrey C. Steinhoff, Managing Director, Financial Management and Assurance, GAO-05-321T, Feb. 16, 2005 (http://www.gao.gov/assets/120/111338.pdf).
16. *Government Auditing Standards 2011 Revision*, GAO-12-331G, December 2011 (http://gao.gov/assets/590/587281.pdf).
17. See sections 3.40 and 3.41 of *Government Auditing Standards* for information on permitted routine activities.
18. See http://www.gao.gov/assets/680/671664.pdf
19. "HIGH RISK SERIES: An Update," GAO-15-290, Feb. 11, 2015 (http://www.gao.gov/assets/670/668415.pdf).
20. "Calling All Government Financial Managers to a More Analytic Role," by David A. Fitz, James P. Hauer III, and Jeffrey C. Steinhoff, *Journal of Government Financial Management*, summer 2015 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2015/aga-data-analytics.pdf).
21. COSO, "Embracing Enterprise Risk Management — Practical Approaches for Getting Started," by Mark L. Firgo and Richard J. Anderson, January 2011 (http://www.coso.org/documents/embracingerm-gettingstartedforwebpostingdec110_000.pdf).
22. "Financial Integrity Act: Inadequate Controls Result in Ineffective Federal Programs and Billions of Dollars in Losses, GAO/AFMD-90-10, Nov. 28, 1989 (http://www.gao.gov/assets/150/148414.pdf).
23. See http://www.gao.gov/fiscal_outlook/federal_fiscal_outlook/overview#t=0

The information contained herein is of general nature and is not intended to address the circumstances of any particular individual or entity. This article represents the views of the authors, and not necessarily the views or professional advice of KPMG LLP.

Jeffrey C. Steinhoff, CGFM, CPA, CFE, CGMA, an AGA Past National President and member of AGA's Northern Virginia and Washington DC chapters, is managing director of the KPMG Government Institute. During a 40-year federal career, he was assistant comptroller general of the U.S. for Accounting and Information Management, led GAO's largest audit unit, had responsibility for developing Government Auditing and Internal Control Standards, and was a principal architect of the CFO Act. He founded AGA's CGFM program and received the Robert W. King Memorial Award, AGA's highest honor. He is an elected NAPA fellow and, in 2006, was recognized as the outstanding CPA in the federal government by AICPA.

Laura A. Price, MA, CGFM, CPA, a member of AGA's Washington DC Chapter, is the lead partner for risk consulting in KPMG's Federal Advisory Practice and an executive fellow of the KPMG Government Institute.

Timothy J. Comello, CPA, a member of AGA's Washington, DC Chapter, is a managing director for risk consulting in KPMG's Federal Advisory Practice and an Executive Fellow of the KPMG Government Institute.

Thomas A. Cocozza, MBA, CGFM, CPA, a member of AGA's Washington, DC Chapter, is a director in KPMG's Federal Advisory Practice and a Fellow of the KPMG Government Institute. He was a charter member of OMB's Office of Federal Financial Management.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 583305

Copyright 2016. Association of Government Accountants. Reprinted with permission. All rights reserved.

About the KPMG Government Institute

The KPMG Government Institute was established to serve as a strategic resource for government at all levels, and also for higher education and not-for-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.

kpmg.com/us/governmentinstitute

For more information, contact:

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

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

Timothy J. Comello
Managing Director, Risk Consulting, Federal Advisory
T: 703-286-8560
E: tcomello@kpmg.com

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

kpmg.com/socialmedia

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 583305