Creating an Integrated Risk Management Approach

By: Bobbi-Jo Pankaj, CGFM, PMP; and Chris Hare, CGFM, CRMA, PMP

Risk Management Through the Financial Lens

Traditionally, internal controls and risk in government have been synonymous with financial concepts such as materiality, accuracy of accounting data and financial statement misstatement. For more than a decade, it has been ingrained within federal, state and local government agencies that the office of the chief financial officer (OCFO), and typically *only* the OCFO, is responsible for assessing internal controls and risk management.

This financial focus has created a perception (and in some instances a reality) in government that non-OCFO personnel are exempt from playing a key role in the internal controls and associated risk management activities that help safeguard government programs. This perception is reinforced by federal laws and regulations. Both the Sarbanes-Oxley Act of 2002, which protected shareholders and the general public from accounting errors and fraudulent practices, and the 2004 revision to the Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*, Appendix A, Internal Control over Financial Reporting,[1] placed increased emphasis in

financial controls over a more holistic enterprise risk management (ERM) approach in order to increase public confidence and transparency in financial management practices and safeguards.

So, how can we move forward from this misconception? First and foremost, it is important to understand internal controls are used to manage both financial *and* program risk. In July 2016, U.S. Controller Dave Mader said program offices should also be aware of internal control requirements, and how internal controls over programs are beneficial to programs, and not just over financials.[2]

Take, for example, a U.S. military veteran who applies for the GI Bill. Before any financial risks associated with monthly payments come into the picture, the veteran must undergo an eligibility determination to assess whether he/she is entitled to receive benefits. Often, the question is asked: Aren't financial controls more significant? In many instances, operational controls are not perceived as key or significant by stakeholders because these controls are not always tied directly to large dollar amounts. Without being able to point to specific dollar amounts, improper payments or other types of financial impacts, it is easy to overlook some of the most

significant operational controls that could wreak havoc in a program were those controls to fail. This applies to the enterprise view, as well, and how these non-financial risks could affect the enterprise risk of the government agency or department.

As a result, the OCFO is often forced to work in a silo regarding the management of internal controls and risk, without the true "buy-in" that is needed from the other program offices and non-OCFO personnel. Although internal controls over financial reporting are important, it is critical to also consider non-financial reporting within internal audit functions as discussed in the Institute of Internal Auditors (IIA) article, "Beyond the Numbers: The New World of Nonfinancial Reporting."[3] By also focusing on non-financial reporting, an organization can create a sound risk-management structure and corresponding internal controls that align to the strategic decisions that organizations make.

Non-OCFO personnel have traditionally not seen the value internal controls and ERM can provide a program office, department, or larger organization; they tend to view internal controls and structured risk management as an additional burden that interferes with program

> **For an agency to truly achieve its internal controls and risk-management objectives, operational risk needs to re-join financial risk on the center stage, per the original spirit of OMB Circular A-123.**

goals and objectives. As defined by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission's *Enterprise Risk Management — Integrated Framework*, ERM is "A process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage

risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Changing Perception

For an agency to truly achieve its internal controls and risk-management objectives, operational risk needs to re-join financial risk on the center stage, per the original spirit of OMB Circular A-123. The prevailing view must be changed to emphasize that internal controls are not a hindrance to programs — but serve to enhance program effectiveness. Although internal controls are frequently perceived as the cause of excessive documentation and additional administrative tasks, internal controls across programs, with the help of the OCFO, can allow a program to reach its objectives, have more effective operations,

better allocated budgets, and have increased control over risk tolerance. In July 2016, Marianne Roth, a branch manager within the office of the chief risk officer at the Transportation Security Administration, said the first step was to change perceptions about risks within the agency.[4] This change in perception, in turn, improves the financial, operational and enterprise risk aspects of a federal agency as risk management is viewed as positive opportunity for preparation as opposed to negative threats to an organization's mission.

In the federal government environment, agencies will have to shift their focus per the updated OMB Circular A-123. Although industry guidance and frameworks had never explicitly neglected the importance of operational risk, the new direction in industry and best practices places increased emphasis on the importance of internal controls and ERM across operational components.

ERM's Focus on Integration (and why it matters to non-OCFO personnel)

So, how does ERM fit into the picture? Governing bodies such as OMB and industry-leading organizations like COSO have either recently updated or are in the process of updating ERM guidance, frameworks and playbooks.[5] It is important for organizations to stay up-to-date with current industry practice to appropriately control risk while maximizing program performance in today's landscape.

The updated OMB Circular A-123 provides new direction for risk management within federal organizations focusing on ERM and the internal controls that support the ERM program as depicted in **Figure 1**. Although this is federal guidance, state and local governments widely

Figure 1. The Non-OCFO Personnel ERM Checklist

- ☑ Provides valuable insight to decision-makers on the effectiveness and efficiency of resources supporting mission-critical and major program operations
- ☑ Increases the likelihood that an entity will achieve its desired objectives
- ☑ Ensures the proper and appropriate linkage between an agency's entity-wide and program-specific strategic plans and objectives
- ☑ Ensures that risks are managed consistently
- ☑ Prioritizes the allocation of resources to the most significant risks
- ☑ Enhances transparency and accountability in overall organizational structure
- ☑ Improves the likelihood of success for strategic planning
- ☑ Increases communication across the entire organization and reduces the silo approach to solving problems that span the agency
- ☑ Creates processes and controls that reduce duplication of effort and maximize limited resources

accept this as a baseline, and there has been a rise in state-government implementations of Green Book-compliant internal control programs. This substantiates the direction of industry best practices and leading frameworks, and shows this should be the focus for risk management going forward. This integration of financial and non-financial, operational risk, and ERM as a whole, brings the traditional internal controls into a much larger entity-wide risk arena.

For there to be successful integration, there must be coordination between the OCFO and non-OCFO personnel for 360-degree risk coverage. The focus on integration not only places an increased focus on both financial and operational controls, but also requires continual coordination between the OCFO and program offices. The OCFO, which has traditionally been the main point of contact for internal control reviews by external auditors, will need to collaborate with the program offices

to successfully meet risk profile and ERM reporting requirements, which will lead to better program performance and outcomes. The OCFO can assist programs by taking control of their own risk profile and risk culture. The OCFO will need to work with the programs to train and prepare them to take increased "ownership" over the state of their control structure and overall risk profile. The benefits of ERM need to be shared and highlighted, and to remind program offices there are key risk areas that may be overlooked if they are only reviewed from a financial perspective. On the website for the state of Utah's Department of Administrative

Services, the department stresses that "An attractive and significant aspect of the ERM process is its capacity for engaging employees in identifying, prioritizing, and solving risks." Getting everyone to realize there is this attractive benefit is key.[6]

Preparing for Tomorrow

Federal, state and local governments alike need to analyze the current ERM environment and agency-wide risks after collecting data through various techniques, including one-on-one interviews; email inquiries; internal and external data calls; and facilitated focus group sessions with designated
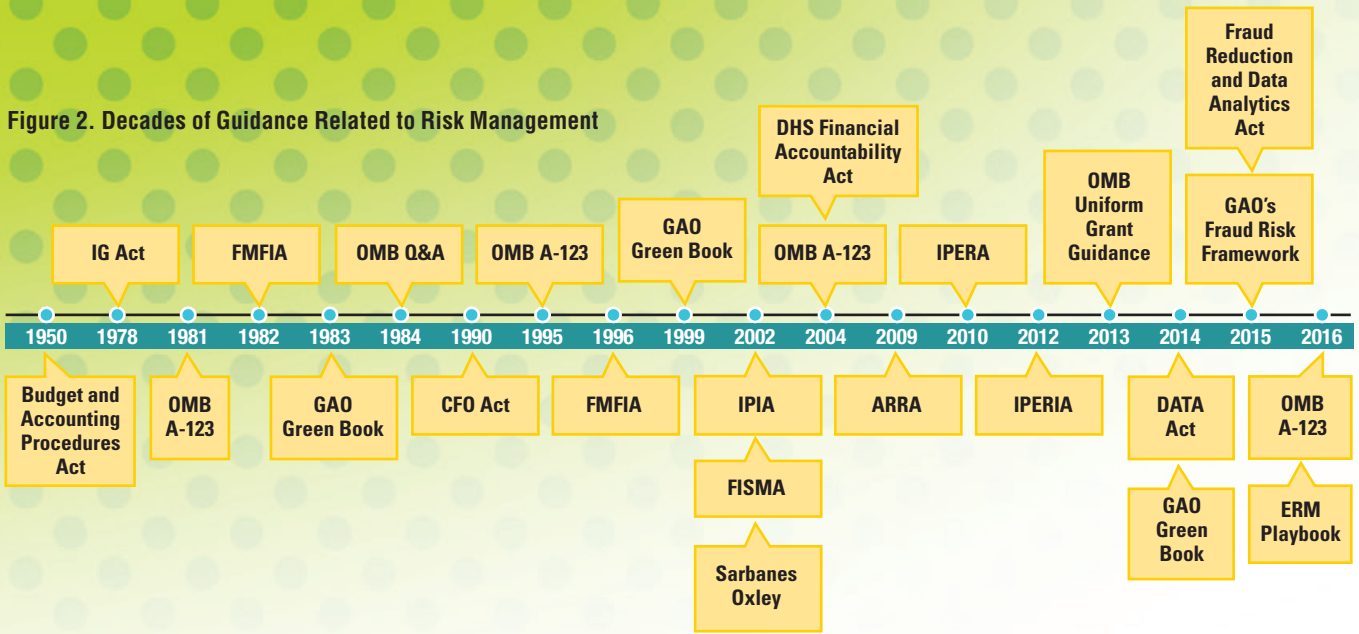
> For there to be successful integration, there must be coordination between the OCFO and non-OCFO personnel for 360-degree risk coverage.

www.manaraa.com

Figure 2. Decades of Guidance Related to Risk Management

Timeline (above line): IG Act (1978), FMFIA (1982), OMB Q&A (1983), OMB A-123 (1984), GAO Green Book (1999), DHS Financial Accountability Act (2004), OMB A-123 (2004), IPERA (2012), OMB Uniform Grant Guidance (2013), GAO's Fraud Risk Framework (2015), Fraud Reduction and Data Analytics Act (2016)

Timeline years: 1950 1978 1981 1982 1983 1984 1990 1995 1996 1999 2002 2004 2009 2010 2012 2013 2014 2015 2016

Timeline (below line): Budget and Accounting Procedures Act (1950), OMB A-123 (1981), GAO Green Book (1983), CFO Act (1990), FMFIA (1996), IPIA (2002), ARRA (2009), IPERIA (2010), DATA Act (2014), OMB A-123 (2016); FISMA; Sarbanes Oxley; GAO Green Book; ERM Playbook

subject-matter experts, key participants and stakeholders.

An article published by the Public Risk Management Association states, "there is always a struggle to get non-risk managers to move beyond their definition of risk management… into a broader application of risk management as a set of principles and tools they could apply to better reach their program goals."[7] There have been great strides made, as illustrated in **Figure 2**, but this is still a struggle in 2016. We need to continue to push to get the topic of risk management and ERM into non-OCFO personnel conversations. The updates to OMB Circular A-123 can help all of us push this concept and embrace ERM going forward.

The legislative environment must also be taken into consideration when evaluating the effects of duplication of effort. Agencies must review various outdated, current and pending legislation, and assess the organization's inclusion and compliance with all requirements on an ongoing basis. For example, updated in 2015, OMB A-11: *Preparation, Submission, and Execution of the Budget*, suggests agencies assess and manage risk as a part of strategic and data-driven reviews in support of the broader organizational risk-management framework, as appropriate for their missions, and in accordance with agency-specific programs. Additionally, agencies should consider compliance efforts that can be consolidated to limit unnecessary redundancies, while satisfying multiple legislative requirements. Preparing for any anticipated legislation allows agencies to remain agile in the event that critical business processes change. A whitepaper on ERM from the Pension Benefit Guaranty Corporation reveals

some important considerations when assessing the current state of an organization's ERM structure, and the importance of adopting best practices, such as "designating the head of a risk organization as a member of executive management."[8] Whether adopting models from the Institute

Figure 3. Developing a Strong ERM Structure

- Address high-risk control gaps with innovative and lasting solutions
- Identify weaknesses and solidify strenghts
- Review relevant frameworks based on up-to-date guidance

A strong ERM structure based on best practices

> We need to continue to push to get the topic of risk management and ERM into non-OCFO personnel conversations. The updates to OMB Circular A-123 can help all of us push this concept and embrace ERM going forward.

www.manaraa.com

of Management Accountants' risk-management maturity model or learning from other ERM cases at other agencies, an organization needs to first internally assess where they stand in order to move forward.

It is imperative that we — financial and non-financial practitioners — review and incorporate best practices within the industry to help get us started in the right direction. Leadership should consistently review industry guidance, leadership surveys and relevant frameworks to determine how to implement the most cutting-edge ERM initiatives. A first step could be to perform a GAP analysis to identify weaknesses and solidify strengths. Management should identify missing, inadequate, or outdated risk-management efforts, strengthen the existing risk-management structure to drive additional value across the agency, and address high-risk control gaps with innovative and lasting solutions (see **Figure 3**).

So, what now? The most important action item resulting from the updated OMB Circular A-123 guidance is we all need to do something and do something now. First and foremost, ERM should be implemented to incorporate the internal control framework and evaluate risk at all levels on a daily basis. While agencies are encouraged to develop their ERM implementation approach now, starting in FY17, agencies annually must develop a risk profile that identifies risks arising from mission support and other operations. The creation of a risk management council (RMC) or inclusion of enterprise risk managers, such as the chief risk officer, to promote ERM and related concepts across the agency, is a good first step to get everyone talking to one another and focusing on how best to create an integrated approach that promotes readiness to address the most pressing risks.

For those of us in the financial community, let's change the perception by showcasing and sharing what we have done around risk management in the financial space with our

> It is imperative that we — financial and non-financial practitioners — review and incorporate best practices within the industry to help get us started in the right direction.

non-OCFO colleagues to prepare for these new requirements and help them get started. This is an exciting time in risk management, and this is something that has not happened in a long time — we are all on this risk-management journey together. 🗗

Endnotes
1. www.whitehouse.gov/omb/circulars_a123_rev; Accessed Nov. 3, 2016.
2. federalnewsradio.com/reporters-notebook-jason-miller/2016/07/123-circular-bring-agencies-back-1980s-around-internal-controls/; Accessed Nov. 3, 2016.
3. The Institute of Internal Auditors, "Beyond the Numbers: The New World of Nonfinancial Reporting," *Tone at the Top*, Issue 75 December 2015.
4. federalnewsradio.com/management/2016/07/tsa-jump-started-enterprise-risk-management/
5. erm.coso.org/Pages/default.aspx and cfo.gov/2016/07/28/enterprise-risk-management-erm-playbook-released/; Accessed Nov. 3, 2016.
6. das.utah.gov/enterprise-risk-management.html; Accessed Nov. 3, 2016.
7. http://des.wa.gov/sites/default/files/public/documents/RiskManagement/PRiMAArticle_20101115.pdf; Accessed Nov. 3, 2016.
8. oig.pbgc.gov/pdfs/ERM-MAR-9-10-15.pdf

Bobbi-Jo Pankaj, CGFM, PMP is a director in the Risk Advisory sub-service line for Grant Thornton's Public Sector. Since 2004 she has led internal control, risk management and ERM engagements for public-sector organizations, assisting them in improving their controls and risk management practices and programs.

Chris Hare, CGFM, CRMA, PMP, a member of AGA's Northern Virginia Chapter, is a senior manager who leads Grant Thornton's Risk Advisory sub-service line and has led a variety of risk management engagements with a focus on the healthcare arena over the past decade.

> The most important action item resulting from the updated OMB Circular A-123 guidance: we all need to do something and do something now.