IBM Center for
The Business of Government

Risk Series

Improving Government Decision Making through Enterprise Risk Management

Douglas W. Webster
George Washington University

Thomas H. Stanton
Johns Hopkins University

Risk Series 2015

Improving Government Decision Making through Enterprise Risk Management

Douglas W. Webster
George Washington University

Thomas H. Stanton
Johns Hopkins University

IBM Center for
The Business of Government

Table of Contents

Foreword 3

Introduction to Risk Management in the Federal Government 5
- What is Risk? 5
- Why Is There Increased Attention to Risk in the Federal Government? 5
- What Is the Value of a Risk Management Focus? 8
- Why Do Agencies Adopt Risk Management Initiatives? 9

Evolution of Enterprise Risk Management in the Federal Government 12
- Traditional Risk Management 12
- Limitations of the Traditional Approach 12
- What is Enterprise Risk Management? 13
- Evolution of Enterprise Risk Management in the Federal Government 15
- OMB Efforts to Encourage an Enterprise Risk Management Approach 17

Challenges to ERM Implementation: Insights from Federal Executives 18
- Challenge One: Sustaining Support from the Top 18
- Challenge Two: Addressing Power Concentrated in Silos 21
- Challenge Three: Overcoming a Culture of Caution 23
- Challenge Four: Reconciling Roles of the Risk Function with Those of the Inspector General or Auditor 24
- Challenge Five: Educating Agency Staff about ERM 27
- Challenge Six: Demonstrating the Value of ERM 29

Six Steps to Successful Implementation of Enterprise Risk Management in the Federal Government 31
- Step One: Establish a Risk Governance Framework 31
- Step Two: Create Conditions for Risk Management to Be Effective 32
- Step Three: Integrate Risk Management into Organizational Decision Processes 33
- Step Four: Protect the Risk Function 33
- Step Five: Build Risk Awareness into the Agency's Culture 33
- Step Six: Manage Organizational Change 34

For Further Reading 35

Acknowledgments 36

About the Authors 37

Key Contact Information 39

Foreword

Daniel J. Chenok

Erica Webber

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, *Improving Government Decision Making through Enterprise Risk Management*, by Douglas Webster and Thomas Stanton.

The public's trust in government continues to be low levels, as measured in numerous surveys. This perception is shaped in part from stories about how federal agencies could have improved, if leaders had taken the time to foresee and mitigate potential risks.

Federal leaders recognize the need to address risks effectively. While historically, the federal government has tended to focus risk management in the financial arena, the Office of Management and Budget has recently launched a major reassessment of the government's approach—encouraging the use of Enterprise Risk Management (ERM).

There are several compelling reasons for the federal government to adopt ERM widely to assess and address risk:

- The approach has been used extensively in the private sector and in other countries.
- There are international standards for its adoption and use.
- These standards are now informing revisions to existing federal risk management policies.

But policies don't readily translate into action. In this report, Webster and Stanton describe the evolution of federal risk management approaches and several agencies' experiences in adopting Enterprise Risk Management. The authors asked current and former federal executives to describe the challenges of adopting an enterprise approach to risk management in their agencies and across the government. The report presents six challenges that they identified and concludes with six steps that organizational leaders can take to make Enterprise Risk Management actionable as a tool for successful implementation of agency programs.

This report builds on a number of previous reports issued by the IBM Center, including:

- *Risk Management for Grants Administration: A Case Study of the Department of Education* by Young Hoon Kwak and Julia B. Keleher
- *Managing Risk in Government: An Introduction to Enterprise Risk Management* by Karen Hardy

In addition, in our 2013 special report *Six Trends Driving Change in Government*, the IBM Center identified the need for a deeper and more nuanced understanding of risk in the public sector.

We hope that the new insights provided by Webster and Stanton are helpful to federal executives in developing actionable approaches to Enterprise Risk Management, especially in advance of pending guidance from OMB on this risk management approach.

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com

Erica Webber
Partner, Finance, Risk, and Fraud Consulting
IBM Global Business Services
eawebber@us.ibm.com

Introduction to Risk Management in the Federal Government

What is Risk?

There are various definitions of risk. Terry F. Buss, an international scholar of public administration, writes, "Risk is defined as the uncertainty of outcomes arising from events, laws, policies, decisions, and actions. Risk has to be assessed against the combination of the likelihood of something happening, and the impact that arises if it does actually happen." He goes on to note that risk is often viewed in negative terms, such as in connection with disasters, but that risk can also refer to positive actions, such as when introducing innovation.[1]

The need for effective risk management in government—and the consequences of a failure to adequately address risk—have become increasingly evident. There are many classic examples of inadequate public and private sector risk management in recent decades, such as the Challenger and Columbia Space Shuttle disasters and the Deepwater Horizon oil spill, to say nothing of the public and private failures that led to the financial crisis of 2007–2008.

We have continued to see an ongoing cavalcade of decisions reflecting poor risk management. The front pages of national newspapers constantly report on actions by private companies, federal leaders, or agencies that do not appear to have considered the risks associated with various decisions and actions. There appears to be a common thread running through these events: a failure to adequately consider risk "up front" and address it as part of an organization's overall management.

Risks come in many different dimensions. The federal government has traditionally focused on managing financial risk, but is now beginning to address risk more comprehensively by incorporating other dimensions. The box on page 6 presents examples of external and internal risk that organizations face.

Why Is There Increased Attention to Risk in the Federal Government?

Assessing risk has long been a management imperative in the private sector, especially in the financial and insurance industries. The federal government has also paid attention to risk that is inherent in selected functions as well, such as natural disaster response and air traffic control. But in recent years, there has been an organic growth in the amount of attention that is being paid to addressing risk across a spectrum of agencies. There are two sets of factors that account for this increased attention: those that are external and internal to government.

1. See: *Evidence-Based Public Management: Practices, Issues and Prospects,* by Anna Shillabeer, Terry F. Buss, Denise M. Rousseau, New York: Routledge Publishers, 2015.

Examples of Types of External and Internal Risks Organizations Face

Hazard risks, such as:

- Liability suits (e.g., operational, products, environmental)
- Fire and other property damage
- Theft and other crime

Financial risks, such as:

- Price (e.g., interest rate, commodity)
- Liquidity (e.g., cash flow, opportunity costs)
- Credit (e.g., default by borrowers)

Operational risks, such as:

- Customer service
- Succession planning
- Cyber security

Strategic risks, such as:

- Demographic and social/cultural trends
- Technology innovations
- Political trends

Reputational risks, such as:

- Procedural and policy mistakes by staff
- Perceptions of misuse of government resources
- Fraud or contract mismanagement

Source: Adapted from Brian Barnier, "Creating and Keeping Your Options Open — It's Fundamental," Chapter 5 in *Managing Risk and Performance: A Guide for Government Decision Makers,* by Thomas H. Stanton and Douglas W. Webster, eds. Hoboken, NJ: John Wiley & Sons, Inc., 2014, p. 123.

External Factors. Environmental factors as diverse as an aging workforce, changing social norms, or increased cyber security threats impact federal agencies in multiple ways. Just as the world in which we live today looks very different than the one in which we lived just a couple of decades ago, the world 20 years into the future will be at least as different. These changes occurring in the external environment outside the organization are the source of numerous risks over which the organization has little to no direct control.

Having limited control over external risks, however, does not mean that they should be ignored. Instead, they must be considered as part of evaluating the achievability of future goals and considering alternative approaches to reaching those goals. Success for any organization—whether public sector, private sector, or non-profit—depends in part on the ability to position itself to provide stakeholder value in the future environment.

Internal Factors. In addition to the risk to mission achievement caused by events and possible changes outside the organization and beyond its control, there are many risks internal to the

organization over which it often does have significant control. The adequacy of internal processes, for example, such as associated controls, training, appropriate organizational values and culture, and many other factors, are under the direct influence, if not outright control, of the organization.

Responding to the External and Internal Environment. As discussed above, risks emanate from both outside and inside the organization. Risks from outside the organization result from changes in the external environment over which the organization may have little or no control, and to which the organization may not be fully prepared to react. Risks arising from inside the organization are potentially within the control of the organization and, therefore, are generally more manageable. While efforts to address external risks can be reactive in nature, there is an added element: the need to proactively anticipate future stakeholder needs and movement in the external environment. This attempt to look into the future and respond to potential future needs requires a more proactive approach to governance and management.

An important distinction between risk generated externally or internally is the degree of planning and proactive leadership required to appropriately identify and manage risks. The management of risks that occurs as a result of delivering current products and services is not a trivial task. It requires an understanding of the resources and processes involved and an understanding of where the uncertainties lie in the delivery of those products and services.

However, management of risks resulting from a changing environment adds the need to anticipate what future requirements stakeholders may have, as well as how the future external environment will affect the organization's ability to meet those evolving stakeholder needs. Effective management requires both process improvement and improved value for today's environment, as well as positioning the agency for the future.

Another factor is the combination of budget uncertainty and budget cuts. Budget uncertainty often reduces the quality of agency decision making. Defending against repeated threats to their budgets can divert the energies of agency managers from their focus on core mission. Distracted managers may neglect important risks that can wreak havoc with their organizations. In her classic study of budget reductions in the 1980s, Irene Rubin found that, "As funding went up and down and the rumors of impending reduction in force came and went, morale went up and down. When morale was low, not only was there no planning, but there was no motivation to make hard decisions. Only the most routine of activities were undertaken."[2]

Budget cuts increase the risks confronting an agency. In both the private and public sectors, major risks have materialized when:

- An organization undergoes a serious reduction in budget
- Top management, for any of a variety of reasons, seeks to "do more with less" without undertaking the necessary work of organizational rebalancing first

In some cases, it simply may not be realistic to expect that an agency can carry out its usual activities in the face of major budget cuts. The essence of strategy is making choices and the agency may need to prioritize its activities and determine which are most important for carrying out its mission.

2. Irene Rubin, *Shrinking the Federal Government: The Effect of Cutbacks on Five Federal Agencies,* New York: Longman, Inc., 1985, pp. 201–202.

What Is the Value of a Risk Management Focus?

Effective use of risk management strategies can improve senior leadership decision making by strengthening both the quantity and quality of the information available for decision making and offering the opportunity for fact-based information flow that can challenge the leadership team's assumptions. There are two important ways in which risk management can be used by an agency's top leadership:

- To strengthen decision making
- To improve information flow

Risk Management as a Tool to Strengthen Decision Making. Decisions, whether to undertake a new initiative or to continue ongoing activities, involve risks and rewards. News about rewards seems to travel quickly to decision makers: proponents of a course of action can usually point to indications, often backed by data of varying quality, suggesting the benefits. By contrast, bearers of news about downside risks are often seen as naysayers and people who "don't want to play," or at least "cheer," for the team. In the federal government, one of the most important questions to ask about a promising new initiative is: "Does our agency have the ability to carry this out?" That also can be one of the most difficult questions for a decision maker to answer.

The world is evolving in ways that make sound decision making increasingly difficult. Technologies make processes, products, and services, increasingly complex. Organizations have also become increasingly complex. Yet it is still possible to make sound decisions in today's environment. Professor Sydney Finkelstein of the Tuck School of Business at Dartmouth University and his colleagues analyzed public and private organizations and their decisions. They found two factors that must be present for an organization to make a major mistake:

- An influential decision maker makes a flawed decision, for any number of reasons.
- The decision making process lacks capacity to provide feedback to expose errors and correct the decision.

The remedy, they concluded, lies with improved decision processes:

- Design the decision process to enlist additional experiences and data relevant to major decisions. This can help to offset tendencies toward group-think.
- Encourage group debate and challenge to ensure that opposing points of view have been heard and understood.
- If needed to avoid chilling the deliberative process, possibly separate the bodies with decision-making authority, with one group deliberating and generating the proposed decision and submitting it to a higher "governance" group for approval.[3]

Risk management plays an important role in such a decision-making process. By institutionalizing the presentation of information about "downside risks" associated with a decision, an executive, such as a risk officer, can facilitate the presentation of important information to help inform the decision-making process. If the agency head or other decision maker can structure a respectful dialogue between individuals responsible for assessing risk and proponents of a new program initiative or other decision, then the agency may be able to find an approach that optimizes the risk-reward tradeoff by borrowing insights from each perspective. A constructive dialogue approach also can be built into a committee structure that incorporates multiple

3. Sydney Finkelstein, Jo Whitehead, and Andrew Campbell. *Think Again: Why Good Leaders Make Bad Decisions and How to Keep it From Happening to You*, Boston: Harvard Business Press, 2008.

perspectives to help all involved to understand the risk-reward contours of important decisions.[4]

Risk Management as a Tool for Improving Information Flow. The quality of organizational decision making improves because effective risk management creates an institutionalized process for encouraging the flow of information across the organization and up the hierarchy to the relevant decision makers. An institutionalized process serves as a buffer against the unpopularity that sometimes plagues an individual who warns about possibilities of failure when agency leadership is charging ahead.[5] Moreover, an institutionalized and well managed risk-management process may help to encourage dialogue, which can provide an opportunity to integrate leaders' goals with the realities of what the agency is capable of implementing.

Benefits of a Risk Management Focus

- Improve the quality of organizational decisions
- Identify major risks before they can grow to unmanageable size
- Clarify risk-reward trade-offs so that an organization can exploit new opportunities
- Improve the flow of information across silos and up and down the hierarchy
- Help the organization to better manage the risks of budget uncertainty and budget cuts
- Prioritize major risks and risk treatments so that an organization can allocate scarce resources to address those that best contribute to organizational stakeholder value

Once information is available, a leader needs to exercise judgment and make decisions about whether and how to proceed. And, not surprisingly, leaders are people too and thus, some have better judgment and management approaches than others. Moreover, in our system of government, agency heads often must juggle a variety of external factors against the information that percolates up from the agencies they lead. Sometimes, for example, external considerations may lead an agency head to call for "full speed ahead." However, once again, the more agency heads understand risks involved, the better equipped they are to deal with them.

All organizations seek to avoid expensive disasters. Many seek to understand the risks that they believe are most important. Many even appoint chief risk officers and task them with investigating risk. But investigating major known risks or appointing a chief risk officer is not the end of the process. Indeed, many organizations that have come to grief have been upset by unexpected types of risk and many of these had risk officers. These experiences reinforce the essential lesson: to be effective (and cost effective) risk management needs to inform an organization at multiple points in its decision-making processes.

Why Do Agencies Adopt Risk Management Initiatives?

In addition to the factors discussed above, federal agencies adopt risk programs for a variety of reasons.

A new leader who appreciates the importance of risk management. This happened with the U.S. Treasury Department's Office of Financial Stability. The incoming agency head, Neel

4. The importance of constructive dialogue was seen in the financial crisis. See, Thomas H. Stanton, *Why Some Firms Thrive While Others Fail: Governance and Management Lessons from the Crisis,* New York: Oxford University Press, 2012.
5. This issue is explored in, Ira Chaleff, *The Courageous Follower: Standing Up to & for Our Leaders,* San Francisco: Berrett-Koehler Publishers, 2009.

Kashkari, came to government from Goldman Sachs, one of the financial management firms that used risk management as the basis for its success in navigating the financial crisis. As he was building out the new office's capability to administer the Troubled Asset Relief Program (TARP), Mr. Kashkari included risk management as a key element in ensuring performance and accountability.[6] Similarly, a new agency head at the Defense Logistics Agency began an Enterprise Risk Management (ERM) program as one of his personal initiatives.[7] These and other examples reflect the lesson that it is often the agency head, or perhaps a strong deputy, who can determine the success of a risk management program.

An organization has suffered losses of resources or reputation, or both, from risks that materialize. There are numerous examples of federal agencies undertaking risk management after encountering a series of problems. For example, Ginnie Mae, an agency that guarantees hundreds of billions of dollars of mortgage-backed securities (MBS), faced a large default when a major MBS issuer failed in the late 1980s. In response, Ginnie Mae created a sophisticated monitoring system, which has now evolved into the Ginnie Mae Portfolio Data Analysis System (GPADS) that produces regular reports on the financial attributes of issuers and lenders that participate in the Ginnie Mae program.

With this type of monitoring, Ginnie Mae can determine the quality of loan origination and servicing of issuers and lenders, compare them against peer institutions, and detect emerging

OMB's Attributes of Effective Risk Management

In its Circular A-11, *Preparation, Submission and Execution of the Budget,* the Office of Management and Budget (OMB) lists the attributes of effective risk management.

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 evolving risk profile of the agency
- Takes human and cultural factors into account
- Is transparent and inclusive
- Is dynamic, iterative, and responsive to change
- Facilitates continual improvement of the organization

Source: OMB Circular A-11, *Preparation, Submission and Execution of the Budget,* Section 270.24, "Performance and Strategic Reviews," August 2014.

6. Harold Barnshaw and Jay Ahuja, "Inside OFS: Managing Risks in a Start-Up Organization," *Risk Professional,* February 2011, pp. 36-39.

7. Jeffrey Stagnitti, "Integrating Enterprise Risk Management with Strategic Planning and Resource Management," chapter 8 in Thomas H. Stanton and Douglas W. Webster, eds., *Managing Risk and Performance: A Guide for Government Decision Makers,* Hoboken, NJ: John Wiley & Sons, Inc., 2014.

risks before they reach unacceptable proportions. Over time, as other risks have revealed themselves, Ginnie Mae has adapted GPADS to take into account additional counterparty issues.

An agency may adopt a focused risk management program as a part of its need to innovate. The Small Business Administration (SBA), similar to other agencies that manage loan guarantee programs, decided in the late 1990s to delegate loan underwriting to banks and other lenders that originate SBA-guaranteed loans. The SBA administrator explained to Congress that risk management was needed to protect against losses from the innovation.[8] The SBA then created an Office of Lender Oversight to monitor the quality of SBA-guaranteed loans that lenders originated under the new program.

Some departments and agencies adopt risk management functions after observing the experiences of others. This has been the case with many organizations that are members of the Association for Federal Enterprise Risk Management (AFERM). First, an agency sends staff to an AFERM or another risk management training event to learn about the elements of risk management and to network with other agency officials who have already established such programs. Then the agency—often acting through its Office of Chief Financial Officer—establishes a small risk function and selects an experienced chief risk officer (CRO). Finally the CRO begins to hire staff to help build out the office and its operations.

8. Statement of Aida Alvarez, administrator, U.S. Small Business Administration, before the Committee on Small Business, United States Senate, Hearing on SBA Credit Programs, May 15, 1997, p. 14 (prepared text).

Evolution of Enterprise Risk Management in the Federal Government

Traditional Risk Management

Traditional risk management includes initiatives that can be described as specialized and targeted. These risk management initiatives largely focus on an agency's or program's internal risks and looks at functional and programmatic operational risk. An example is Ginnie Mae's creation of the GPADS monitoring system in response to a specific failure as discussed on page 10.

Traditionally, risk has been managed within relatively narrow domains. These domains may be functional in nature, such as risks associated with responsibilities of the chief financial officer, chief information officer, or other functional areas. Risks are also addressed within programmatic domains, such as within an agency's or bureau's particular programs or projects.

All programs, functions, and other organizational elements have objectives related to their roles in the organization. They also have risks in achieving those objectives. Understanding and managing these risks typically requires specialized knowledge and experience relevant to the objectives sought and the risks encountered. Avoiding the risks of a failed financial audit, for example, requires individuals with the proper training and background to understand finances, Generally Accepted Accounting Principles (GAAP), internal controls, and other skills needed to ensure a well-functioning financial system. Similarly, protecting the organization from Internet security breaches requires proper training and experience, using relevant technologies and best practices.

In short, effective functional and programmatic risk management requires skills and experiences that may be very specific and narrowly focused. Nearly all government organizations manage such functional and programmatic risks at some level. Moreover, much of the role of OMB and the Government Accountability Office (GAO) is to help bring such functional risk management practices to at least a minimum level of acceptability.

Limitations of the Traditional Approach

No matter the degree of sophistication in managing functional risks, shortcomings can easily remain when risks are managed in one functional or programmatic area, independent of risks in other programmatic or functional areas. These shortcomings can present themselves in a number of ways.

Gaps in the identification, assessment, and treatment of risks between functions, programs, or organizational subdivisions. Because often no single individual is responsible for management of risk within various areas of the "white space," these risks can easily exist without

being ever being identified—until, of course, those risks turn into adverse events.[9] Raising consideration of risk management through and beyond the functional and programmatic silos within which it traditionally has operated allows for consideration of risks that may exist in such "white space" outside the silos.

Inefficiencies due to overlaps in the treatment of shared risk. In contrast to gaps in the coverage of risk management, one might reasonably assume that overlaps in risk management by different parts of the organization are not problems, but this is not the case. The problem with overlapping actions for particular risks is twofold:

- The duplication of effort, even in the best of cases, by different parts of the organization working independently of one another is an inefficient use of resources.
- Actions taken to address a risk in one part of the organization may conflict with those taken in another part of the organization.

Inconsistencies in the treatment of risks by various functions due to dissimilar risk appetites and approaches to risk management. Another source of inefficiency occurs when different parts of the organization are left to develop their own approaches to risk management without any central guidance. In such an environment, it is likely that some elements of the organization will develop stronger risk management practices than other parts of the organization. While one part of the organization may implement widely recognized best practices, other parts of the organization may struggle to implement even minimal risk management practices. Moreover, parts of the organization will inevitably be more risk tolerant or risk averse than other parts of the organization, without any rationalization for those differences.

Lack of strategic alignment. All parts of the organization, regardless of their functional or other contributions, need to be aligned with organization-wide goals to maximize their contributions to the ultimate objectives. Subordinate parts of the organization that do not so align their efforts in creating value for organizational stakeholders ultimately use up resources needlessly that degrade the value of products or services delivered. As strategic goals cascade down into subordinate, supporting goals and objectives, so too do associated risks to achieving them. Organizations that fail to understand how risks relate to objectives as they cascade down from enterprise goals into functional, business unit, and program goals, will not effectively address risks to those objectives.

Reduced return on investment in the application of limited resources to the delivery of a portfolio of products and services. These limitations in traditional risk management by functional or programmatic silos lead directly to failure to identify and manage risks in the most cost-effective manner. Risks existing in the "white space" may easily be missed. Duplication of risk management efforts in different parts of the organization to address common risks can easily result in the inefficient application of resources, and at worst, conflicting risk treatments that actually create new risks.

What is Enterprise Risk Management?

Often, the risk that hits an organization hard may not be the one that the organization was anticipating. As organizations have become more experienced in the application of risk management, the shortcomings of the traditional siloed approach to managing risks within functional and programmatic silos have become more obvious. This has led to slow but ongoing

9. "White space" is a term coined by Geary Rummler and Alan Brache as the area between the boxes in an organizational chart, where, very often, no one is in charge.

progress toward implementing the principles of Enterprise Risk Management (ERM). One of the earliest formal definitions of ERM was introduced by the Casualty Actuarial Society (CAS). In a report by its Advisory Committee on Enterprise Risk Management,[10] the CAS in 2001 defined ERM as follows:

> ERM is the process by which organizations in all industries assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organization's short and long term value to its stakeholders.

More recently, AFERM defined ERM as:

> … a discipline that addresses the full spectrum of an organization's risks, including challenges and opportunities, and integrates them into an enterprise-wide, strategically aligned portfolio view. ERM contributes to improved decision making and supports the achievement of an organization's mission, goals, and objectives.

These definitions are instructive, in part because they point out that ERM is more than simply "good" risk management as traditionally practiced in silos. The AFERM definition references "the full spectrum of an organization's risks," while the CAS definition cites risks "from all sources." These definitions inherently require a top-down, strategically driven approach to risk identification. The problem of "white space" means that such a comprehensive view of risk will not emerge simply from a bottom-up aggregation of risks identified within functional and

What Are Some of the Distinguishing Characteristics of ERM?

The Risk and Insurance Management Society (RIMS) has identified seven characteristics that yield insight into what constitutes ERM:

- Encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc.)
- Prioritizes and manages those exposures as an interrelated risk portfolio rather than as individual "silos"
- Evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances, and stakeholders
- Recognizes that individual risks across the organization are interrelated and can create a combined exposure that differs from the sum of the individual risks
- Provides a structured process for the management of all risks, whether those risks are primarily quantitative or qualitative in nature
- Views the effective management of risk as a competitive advantage
- Seeks to embed risk management as a component in all critical decisions throughout the organization

These characteristics clearly distinguish ERM from those practices that are sometimes incorrectly understood to be ERM.

10. Jerry Miccolis, et. al., *Final Report of the Advisory Committee on Enterprise Risk Management,* Casualty Actuarial Society, Nov. 5, 2001

programmatic silos. The need to incorporate risk management into the strategic planning process is an inherent part of any meaningful ERM program, and this, again, requires a comprehensive view of major risks to the agency and its programs.

Another shared aspect of these definitions is that they position ERM, not as an end unto itself, but rather as an element of a broader objective. Risk management is simply an element of effective organizational management and the AFERM definition reflects the tie of ERM to improved decision making and the achievement of the organization's mission, goals, and objectives. The CAS definition indicates that ERM leads to increased short- and long-term value. Finally, the AFERM definition indicates that ERM enables a portfolio view of organizational risks. Just as a portfolio of personal financial investments is intended to maximize the risk-adjusted return on investment for retirement planning, so too, treating an organization's array of products and services, and balancing resources against performance objectives and risks across that portfolio of products and services, serves to maximize long-term organizational stakeholder value.

Evolution of Enterprise Risk Management in the Federal Government

While the concepts of ERM outlined above have been maturing in the private sector for the past two decades, their introduction into the public sector is more recent. What is believed to have been the first enterprise-wide implementation of ERM in the federal government can be found at the Office of Federal Student Aid (FSA) in the Department of Education. In 2004, FSA hired a CRO, Stan Dore. Mr. Dore is believed to have been the first person in the federal government to fill this position. FSA formally approved the creation of a dedicated Enterprise Risk Management office early in 2006. Since those initial efforts, FSA has continued to mature its ERM processes and organization.

In 2008, Doug Webster, a co-author of this report, was serving as the chief financial officer (CFO) of the U.S. Department of Labor. With a strong belief in the value of ERM, he reached out to other federal executives who shared that interest. Early in 2008, this informal group established itself as the Federal ERM Steering Group and joined with George Mason University to convene the first Federal ERM Summit. That annual event has been held every year since and has become the key event for bringing together those interested in ERM in the federal government. In 2011, the Federal ERM Steering Group was formally incorporated as the aforementioned Association for Federal Enterprise Risk Management (AFERM).

Despite the impetus provided by AFERM and its annual Federal ERM Summits, progress in the federal government was initially slow. In the Association for Government Accountants' Annual CFO Survey in 2010, five federal executives were noted as having a formal risk management process in their agencies, including the designation of a chief risk officer to facilitate ERM. While this certainly represented progress from FSA's initial appointment of a CRO, the surveyed organizations represented a small portion of the federal government. Moreover, meaningful progress was impeded because conflicting messages were being sent about the true meaning of ERM. For example, in the 2011 CFO Survey conducted by the Association for Government Accountants, 50 percent of respondents indicated that they believed that ERM was adequate in their entities. However, one respondent stated, "We have risk management committees of senior executives and subject matter experts aligned with each portion of our financial balance sheet. They recommend actions to a national risk committee to evaluate the risks." This reflected a common misunderstanding of the differences between a functional risk (e.g., financial reporting) and meaningful ERM.

What is an Enterprise?

The question that often arises in ERM is the meaning of "Enterprise." Must ERM be applied at the departmental level to qualify for that term? Can ERM be applied within a bureau even if the parent organization does not implement ERM principles? Can ERM be applied within a functional business area, such as financial management or information technology?

The authors of this report contend that ERM is about the application of a set of guiding principles, and not whether or not the organization within which ERM is implemented is itself a subordinate element of a larger organization. For instance, ERM could be effectively applied across the U.S. Coast Guard or the Secret Service even if it was not fully implemented at the Department of Homeland Security level.

In keeping with the above, it is thus possible to implement ERM within a program or large functional unit. However, ERM is ultimately about the implementation of key principles, and not the size of the organization or its relationship to a parent organization. Even if the Department of Defense did not adopt ERM, this would not preclude a garrison commander at an Army installation from implementing ERM effectively.

While the principles of ERM may be applied within a functional area to manage risk (such as impacts to reliability in a balance sheet), this does not represent the principles of ERM applied across an agency. This same study revealed that only 29 percent of respondents indicated there was a designated risk management office or operation in their agencies. Given the lack of a central coordinating risk management office, this begs the question of whether a meaningful ERM program was in place. As the authors of this report have sought to explain in describing ERM, there is a need for a central office or function generating centralized risk management policy, establishing cross-functional risk management processes, facilitating collaborative risk management discussions, and prioritizing risks.

While in 2011, the term ERM may have been more broadly recognized than the understanding of the underlying concepts, organizations have sought to improve on that understanding. The Winter 2013 edition of the *Armed Forces Comptroller*, the journal of the American Society of Military Comptrollers, focused largely on ERM, thereby helping to spread the word on the principles of ERM in that community. An additional effort aimed at helping inform the federal community about ERM principles and practices was the publication of the book *Managing Risk and Performance: A Guide for Government Decision Makers* (Wiley, 2014), co-edited by the authors of this report.

Despite the initially slow progress and misunderstanding of the term ERM, concrete progress is now demonstrably underway. In the book just referenced, the last of 10 recommendations offered for the federal government was to "incorporate ERM explicitly into Circular A-11 and OMB reviews of agencies." On July 25, 2014, OMB released an update to Circular A-11 (its annual guidance to agencies on the preparation of their budget submissions) that recognized ERM as an important practice for managing agency risk.

OMB Efforts to Encourage an Enterprise Risk Management Approach

OMB's current interest in ERM has evolved over time, but became more evident early in 2013. OMB began working with the GAO to provide input on an update to Standards for Internal Control in the Federal Government ("The Green Book"), and to consider how evolution of the Green Book might influence internal controls policy reflected in OMB Circular A-123, *Management's Responsibility for Internal Control*. With the release of the exposure draft on internal controls by the GAO in the fall of 2013, OMB sought to encourage a more robust consideration of risk management than the check-the-box compliance attitude sometimes seen in federal agencies. The awareness of ERM was at least partly responsible for the effort to move beyond a focus on internal controls in A-123 to a broader view of risk management. The next version of A-123 (at the time this report was published) is thus expected to broaden the role of A-123 beyond internal controls to include other aspects of risk management.

In parallel with these developments, in 2013, OMB asked the CFO Council for suggestions on what OMB and the CFO Council might focus on as initiatives in the coming year. The number one suggestion from the CFO Council was ERM. CFOs felt they were doing a good job of financial management and risk management within financial management, but were struggling with other types of risk. OMB thus started a working group on ERM under the CFO Council. One result of this working group was to convene a CFO Council forum. This forum had most of the CFO Council in attendance and was both an educational discussion on the meaning and practices of ERM, and a discussion of next steps in the council's engagement with ERM.

In October 2014, David Mader, OMB controller, stated in a panel discussion that:

> We have begun talking about how do we think about risk more broadly than just financial risk? I think when you look at [Circulars] A-11 and A-123, those were all borne out of the CFO Act. So everyone is narrowly focused on 'well, it's about financial risk and it's about internal controls.' What we are doing now is stepping back and thinking isn't there really a way to take the lessons learned and what we've accomplished with A-11 and A-123 and broaden that perspective across the entire organization, particularly around mission programs.

Mader went on to state that OMB believes there needs to be an enterprise risk protocol across government, and that OMB would provide that guidance late in 2015.

Challenges to ERM Implementation: Insights from Federal Executives

In preparing this report, the authors interviewed senior leaders in the federal government who have either:

- Implemented ERM
- Are in the process of implementing ERM, or
- Are strong advocates of ERM

To ensure open and free exchange, the identity of these individuals and their organizations has been protected. However, their insights and experiences provide valuable information to be considered by any organization that seeks to better understand and manage enterprise risk. This section presents the challenges the federal government faces in implementing ERM. The list of challenges is especially interesting because it reflects the views of risk managers who are actively grappling with a variety of obstacles as they work to improve their agencies' cultures and practices.

ERM poses basic challenges that must be addressed before it can become ingrained in an agency's processes and culture. Our interviewees identified six challenges that need to be overcome in the implementation of ERM. Four of these challenges relate to the distribution of power within the organization and two relate to conceptual issues and basic understanding of ERM.

Challenges relating to the distribution of power in an agency:

- **Challenge One:** Sustaining support from the top
- **Challenge Two:** Addressing power concentrated in silos
- **Challenge Three:** Overcoming a culture of caution
- **Challenge Four:** Reconciling roles of the risk function with those of the inspector general or auditor

Challenges relating to basic understanding of ERM and its value:

- **Challenge Five:** Educating agency staff about ERM
- **Challenge Six:** Demonstrating the value of ERM

Challenge One: Sustaining Support from the Top

Understanding the Challenge

Interviewees repeatedly raised this as an issue. Perhaps the clearest indication of the importance of support from top leadership came from an official who saw one agency head build a strong ERM capability in the agency, only to be followed by a new agency head who had other priorities.

Implementing ERM in Federal Agencies: Progress to Date

Officials at many agencies reported progress in implementing risk management, as well as ERM. Progress ranges from taking first steps toward ERM to developing a fairly robust ERM process.

- **Moving Beyond Internal Controls.** One organization developed a robust internal controls program in response to past problems highlighted in a Government Accountability Office (GAO) report. With the arrival of a new chief financial officer (CFO), it was decided that the organization needed to move beyond internal controls toward a more comprehensive risk management program. A senior advisor to the CFO was appointed specifically to roll out an ERM program. The initiative to implement ERM was a major cultural shift for the organization, which was very decentralized. As the senior advisor reported, "Any organizational element could have become fodder for the *Washington Post*." Thus far, the program described above is in its early phases. The risk staff have identified major risks, provided leadership briefings, and gained buy-in at the executive level. An enterprise risk committee with 13 members was formed that has an enterprise-wide view. The committee reviews enterprise risks and directs deeper dives from functional units when required.
- **Creating a Chief Risk Officer.** A chief risk officer (CRO) at another agency reports directly to the deputy commissioner for finance and administration, but also has an agency-wide role. She views her role as partly one of educating the organization on the value of ERM, and thereby making the case for change that she is helping to lead. She described key products of ERM as the:
  - Ability to present comprehensive analyses on the most significant operational (e.g., IT, HR, business process, etc.), reputational, and strategic risks an organization faces
  - Ability to present analyses of how risks can impact one another
  - Identification of common root causes, which is enormously valuable in helping organizations reduce the likelihood of risks and potential adverse impacts

  This organization is still early in its journey toward full ERM implementation. Officials are building a formal risk appetite statement, which they believe is important as a check point for considering various actions and programs. They have established a common risk lexicon through the organization's Enterprise Risk Management framework. They are in the process of finalizing organization-wide risk reporting mechanisms and risk assessment reporting. Such reporting supports a shared understanding of the most substantial risks the organization faces and facilitates the sharing of lessons learned across the breadth of the organization.
- **Getting Off the High Risk List.** An official at another organization, which had been on the GAO High Risk List for a long period of time, reported that the secretary of the department wanted the organization off that list. This interviewee, who served as the agency's risk officer, believed that ERM could be a means of achieving the secretary's objective. The agency did get off of the high risk list in a year and began to help build an organizational culture that understood and valued ERM.

  In that same organization, an office to lead agency risk management was established and the journey toward ERM implementation was undertaken. Today, ERM staff are sitting in on meetings to understand risks and develop draft risk identifications. These risks are coordinated with functional staff to develop a draft risk register, and are in turn formalized at the risk management committee meetings.

The examples presented above represent instances in which ERM is taking hold in the federal government.

In this example, the interviewee reported that the previous agency head had arrived with an understanding of the principles of ERM and then set about developing both the organizational culture and the training needed to understand, accept, and employ ERM. During this agency director's tenure, major progress was made on the journey to implement ERM.

The interviewee reported that changing and institutionalizing a new organizational culture takes time. While this agency leader brought the understanding and initiative to begin the process of implementing ERM, he did not have the necessary time in that position to fully institutionalize the change. Such institutionalization would have required, among other things, setting in place all of the supporting policies and processes, and linking required actions to executives' and managers' performance plans.

When this agency leader left the organization for a new position, his replacement arrived with a new set of priorities that did not include sustaining the objectives of his predecessor. The new agency head arrived with an agenda to cut costs. This cost-cutting agenda was not linked to a strategic planning process, and entailed very limited discussion of balancing costs, benefits, and risks. In such an environment, the consideration of risk became much less important for top management.

Responding to the Challenge

In an initial substantive discussion with a new agency head, agency staff should emphasize the importance of risk management, the implementation of which can enhance a new leader's reputation and ability to carry out his or her agenda at the agency. In that same discussion, it should be mentioned that vulnerabilities that might have been created under a former agency head can cause harm for his or her successor. It is, therefore, in the new agency head's best interests, as an exercise in due diligence, to review the agency's vulnerabilities and the quality of the processes it has in place to identify those risks.

If such due diligence is not undertaken, the new agency head's tenure could be damaged if something unexpectedly blows up. Moreover, even if new agency leadership chooses to shift to a new set of objectives, delivering on them entails a degree of risk. While the risks to those new objectives may well be different than the set of risks associated with prior leadership's objectives, the need for and value of effective risk management is just as great.

A second response to this challenge is to point out to the new agency head that risk management has now become a priority for the Office of Management and Budget (OMB) and GAO. An agency is well advised, therefore, to act proactively by building its own ERM capabilities and, thereby, forestalling adverse reviews from oversight bodies and even the agency's own inspector general. Here too, the agency head's personal reputation may be at stake.

Third, it is useful to point out to a new agency head that ERM is an integral part of good management and that the agency head can delegate leadership of the ERM function to the agency's chief operating office (COO) if the new agency head has other priorities.

Fourth, agency staff can stress that ERM plays a particularly important role in helping to manage a program of cost reduction. ERM provides an effective process for an agency head to focus cost cutting on lower priority activities while protecting the basic capacity of the agency to carry out its mission without a costly failure, such as has occurred at a many agencies that cut their budgets unwisely.[11]

11. Thomas H. Stanton, "Risk Management and the Dynamics of Budget Cuts," Chapter 10 in Thomas H. Stanton and Douglas W. Webster, eds, Managing Risk and Performance: A Guide for Government Decision Makers, John Wiley & Sons, Inc., 2014, presents a number of examples.

Challenge Two: Addressing Power Concentrated in Silos

Understanding the Challenge

This was a challenge of concern to a number of interviewees. At one agency, despite a degree of understanding and commitment at the highest levels, there is much less buy-in at lower levels in the organizational structure. While decentralized and siloed agencies are certainly not unique, many individuals throughout government have never worked at another agency. As a result, change is often not readily accepted.

In another agency, a challenge to early-stage ERM was the traditional strategic planning process. The agency followed OMB Circular A-11 to produce a plan with strategic goals and objectives. However, the interviewee indicated that strategic planning was primarily a budgeting process that was designed to align existing programs with high-level goal statements. His sense was that individual programs were largely addressed separately, rather than through a holistic enterprise-wide process that addressed both administration and agency leadership priorities, as well as the various risks that the agency must address to ensure efficient and continuously effective operations. The interviewee also indicated a sense that some managers are most focused on the effectiveness and efficiency of their own programs rather than considering first and foremost what is in the best interests of the agency overall. Such thinking can be the cultural norm for many traditional, siloed government organizations.

The problem that must be overcome is the limited incentives that now exist to encourage working across silos. In the public sector, organizational objectives are often less measurable because of a lack of a profit objective. As a result, subordinate organizational objectives can take priority over more abstract enterprise mission objectives, resulting in a stronger focus on achieving the former, without particular regard to the latter.

Responding to the Challenge

Support from the top of the agency can overcome business unit heads' resistance to thinking about risks beyond their own silos and can encourage collaboration to address risk on an enterprise-wide basis. A number of interviewees noted their agencies' success in addressing the challenge silos pose. There are several approaches that agencies have used to respond to the silo issue.

Approach One: Focus on a Limited Number of Risks

One approach to overcoming this challenge is to focus on a limited number of risks that the agency recognizes as being important. One interviewee, an operational risk manager, is working with agency leadership to take a more integrated approach to operational risk management across the entire organization. While limiting the scope of an integrated risk management program to operational risks does not constitute ERM, it does nevertheless demonstrate the collaborative, cross-functional risk management processes that are essential to ERM. Moreover, a more integrated approach to operational risk is enabling the business units to become more comfortable with a collaborative approach to risk management—a capability that will be essential as the agency begins the move to ERM.

Approach Two: Create Risk Management Committees

Another organization, similar to many in the federal government, has suffered reputational impacts due to very public failures of institutions over which this agency has regulatory authority. As a result, the organization is moving increasingly quickly to improve its internal risk management capabilities. The organization has yet to head down the road to implementation of ERM, however. ERM was viewed as a "massive" undertaking and the organization needed to

start smaller to get wins and convince various stakeholders of its importance. Further, the organization is not staffed for ERM and has started by hiring a small Operational Risk Management team. There is currently in place a risk management committee with representatives from many of the approximately two dozen subordinate organizational units. While the risk management committee focuses only on operational risks, it is building the value proposition of collaboration and of sharing risk information.

One process the risk committee evaluated was cybersecurity. Through this process, the chief information security officer was able to communicate the vast array of activity to executives in the front office who did not understand the full scope of the back office's activity. In addition, identification and assessment of cyber risks across business units permitted the identification of best practices and knowledge sharing related to data security risks and mitigation plans unique to multiple business units. For all participants, this helped to make the case for a collaborative approach to risk management, and for developing a portfolio view of risk.

Approach Three: Limit the Size of Risk Management Committees

Another approach is to limit the size of the executive risk committee. While this approach illustrates the potential value of an enterprise-wide, collaborative approach to risk management, there is still often significant pushback from parts of the organization. While leadership in one agency initially sought to have very broad representation in the risk management committee, inability to achieve consensus on top agency risks from a large committee of executives resulted in a decision to reduce the committee to a smaller number of representatives from key business units. The agency found the smaller executive risk committee to be a more effective means of beginning to develop its risk management capability.

Approach Four: Institutionalize ERM

Another approach is to institutionalize ERM and, increasingly, bring senior executives into the process. Because government employees are often less motivated to work toward higher "team" goals (i.e., agency mission is often less a driver for individual performance than subordinate organizational priorities), communications from the top play a particularly important role in moving the organization to a more collaborative operating model. Individuals leading the risk management initiative must recognize the importance of institutionalizing key policies and processes if the initiative is to survive the retirement or other departure of senior risk management champions.

One organization is putting in place governance structures that have begun to help institutionalize ERM concepts. As the risk committee continues to review top agency risks, additional senior executives are coming on board who support the value of risk transparency and ERM. As the agency decides to move toward ERM, it is also assumed that bringing in additional people at a senior level who understand ERM will be helpful.

Approach Five: Tie the ERM Process to Budget Allocation

Another effective approach is to tie the ERM process to the allocation of budget resources. One organization actually rewarded subordinate organizational elements for bringing risks forward by providing additional resources to address risks, either through business process improvement resources, or through the budget process. The motivation for identifying and sharing risks is a budget allocation process that incorporates consideration of risk and risk mitigation. If a subordinate organizational element claims to have zero risk, it may have too high a budget. Theoretically, the budget would be reduced for that organizational element until the level of risk is commensurate with that of the rest of the parent organization. At this agency, risk management is tied directly into the budgeting process.

Approach Six: Create a Culture of Trust

In the final analysis, a culture of trust is needed to overcome the control of information by business unit heads so that they are willing to reveal their vulnerabilities without being penalized for bringing the news to top management. This issue permeates challenges to good management and several of the challenges to effective ERM in particular.

Approach Seven: Work Closely with Business Units

One organization that is farther along than most reported that its biggest success has been in working with the various business units of the organization to help them identify their largest risks. In particular, this organization has worked with business unit partners to improve business processes, which has helped them to improve their consideration of how to balance performance, cost, and risk to optimize stakeholder value. Once business unit leaders understand that the risk management organization can be a partner that can add value to the program, and not a roadblock or gatekeeper through which they must pass, a joint partnership with the business units becomes possible.

Challenge Three: Overcoming a Culture of Caution

Understanding the Challenge

An unexpectedly large number of interviewees identified the need to overcome a culture of caution as a major challenge. It was reported that overcoming the limited appreciation for risk management and the lack of risk management processes is made more challenging because there is often a sense that the risk/reward tradeoff in the public sector encourages avoidance of risk. For many individuals, the belief is that the rewards for taking a chance and achieving success are inadequate compared to the downside of adverse risks becoming reality. To avoid reputational risk or even the possibility of termination or involuntary reassignment, the preferred course of action is often to:

- Avoid taking initiative because you will be punished if you are not successful
- Do only what you have to do

These are obviously misaligned incentives, but, when combined with siloed information and responsibilities, they compound one another. In such an organizational culture, individuals care about "their job," but often do not appear to care about anything that is outside their personal responsibility. Federal agencies have too often found themselves defending their actions on the front page of the newspapers as a result of such an unproductive organizational culture.

In public sector organizations, individuals have historically stayed "out of trouble" by complying with laws and regulations. Many public sector employees have been content with the status quo because of risk-reward tradeoff considerations. Private sector employees may be motivated to respond differently, however. It is often pointed out that the federal government does not have the profit-and-loss pressures the private sector faces. As a result, the public sector is usually not driven to "optimize" to the extent found in the private sector.

While some federal organizations have high visibility and can quickly be called to task by the public, OMB, Congress or other stakeholders, much of the federal government operates as a "back office" function with limited public visibility. Too often, the attitude of some employees in such organizations is to do what is required simply to get by; not to—as another interviewee noted—"rock the boat." Partly because of this attitude, there is also often a culture of not wanting to share bad news, or worse yet, news of non-compliance and poor performance.

Specialization is rewarded, so there may be little incentive for federal employees to think broadly. However, overspecialization and a failure to take a broad view can have adverse consequences.

One agency faced a challenge to develop processes and incentives to facilitate a risk-aware culture in which risk identification was rewarded and valued. The risk officer reported that line employees sometimes see risks of which management is unaware. Lower levels of management may see risks that are not brought to the attention of the executive team. Risks cannot be effectively prioritized and addressed through resources assigned for treatment if they are not first identified and reported. This risk leader recognized that having processes in place to identify risks would be meaningless if the individuals in the organization did not feel motivated and encouraged to report those risks.

A former chief risk officer, who has since moved to a broader operational role, observes that it is disturbing that one organization after another finds itself facing major negative issues/events with no prior notice provided to leadership. Good risk management helps to overcome this problem, as does an organizational culture that is transparent and does not "shoot the messenger." Another interviewee saw it as a challenge to have individuals realize that the risk management initiative is not about criticizing past results, but rather helping to further improve future results through a more robust understanding of risks in achieving objectives.

Responding to the Challenge

Again the tone from the top is essential. Employees must trust that they can safely report risk-related information. In the end, such reporting must be seen as a component of orderly conduct of agency business rather than a sign that a particular employee is "rocking the boat."

To further encourage the sharing and transparency so critical to ERM, some organizations have been explicit about the importance of sharing risk information, and of not "shooting the messenger" when risks are identified and brought forward. An organization must have the necessary degree of transparency to allow those who see the signs and identify the risks to inform leadership, a degree of accountability across all levels of the organization to report risks to senior management, and a leadership that understands the importance of managing risks once they are identified. An ERM program that is institutionalized within an agency can be of great assistance to both political leadership and career executives in identifying and managing risks that, if ignored, will come back to haunt the organization and their time in office. A risk officer reported that the need for very senior managers to deliver this messaging is critical due to the hierarchical structure of the organization.

Challenge Four: Reconciling Roles of the Risk Function with Those of the Inspector General or Auditor

Understanding the Challenge

Several agencies have reported difficulty reconciling the roles of risk managers and those of auditors and especially the staff of the Inspector General (IG). The quality of working relationships between the IG staff and the respective agency are of paramount importance. The Inspector General Act of 1978, as well as subsequent amendments, have provided IGs with sweeping powers to investigate waste, fraud and abuse. Some IGs have used this power to establish independent yet positive working relationships with their agencies to ensure, not only that fraud and abuse are kept in check, but that waste and inefficiencies are identified in a manner that allows the agency to benefit through improved decision making. Some agencies

fear, however, that their IG staffs are more interested in finding fault with past management actions than in a positive effort to improve future results.

A positive yet independent relationship between the agency and its IG can help to bring needed decision-making quality to a federal agency. By contrast, when such a positive relationship does not exist, requests from IGs for pre-decisional information on risks and potential risks can have a chilling effect on efforts to develop the degree of transparency and open dialogue that is essential to any risk management initiative, and particularly one focused on ERM. It is entirely appropriate for an IG to review and assess the quality of an agency's risk management and its risk management function. However, if an adversarial culture exists between the IG and organizational leadership and if the IG uses insights gained from the agency's risk management function to suggest that the existence of risks automatically implies management failures, then this will chill the flow of risk-related information to the risk office and top management. If people believe that, by recording risks those records will be used against them, they may simply choose not to document those risks. This then becomes completely counterproductive.

Encouraging agency officials and employees to share sensitive information about vulnerabilities is one of the most important activities of a risk office. In an organization with a positive working relationship with the IG, selective use of information from the risk office can inform the audit process and help focus on value-added areas where risks may not be as well understood and managed. If, however, such agency risk-related information simply becomes a vehicle to criticize the organization for not having eliminated all (or even most) risk, it can impede frank communications and make effective ERM difficult or impossible. This concern is not only in regard to IG reports, but also to public requests for information. For example:

- Concern had been expressed by some parts of one organization that identifying and documenting risks could become subject to Freedom of Information Act (FOIA) requests, inspector general and congressional requests, etc. The underlying issue was that a requirement to disclose risks would serve as a disincentive to identifying and documenting risks. This organization sought guidance from its general counsel, who stated that FOIA exemption #5 would allow the agency to not disclose such data externally. This exemption for FOIA relates to documents that are part of the agency's "pre-decisional" deliberative processes.
- Despite its progress, another agency continues to be challenged by issues of transparency. While seeking to facilitate transparency and a collaborative approach across functional silos, the agency continues to resist sharing this information with auditors. Whether or not this lack of transparency with auditors and other external parties is beneficial to the organization is a matter of debate.

Another interviewee provided a more general view of the need to protect the flow of risk-related information. This interviewee offered a word of caution related to the challenges in creating a "safe" environment in which management can have candid discussions, while maintaining an appropriate level of transparency that is required of public institutions. Achieving organizational objectives in the public sector is frequently made more challenging than in the private sector because there is much less unanimity regarding goals and priorities among external stakeholders. Leadership must balance the ability to achieve mission goals and objectives handed to it by higher leadership or the White House, while encouraging and demonstrating internal accountability and transparency. The conversation the government risk management community is having—how to create a "safe" environment in which top management can encourage these candid discussions—is critical to creating a risk management culture of transparency.

Responding to the Challenge

Constructive dialogue between an agency's risk officer and its inspector general is essential. In a process of constructive dialogue, the parties seek to optimize their respective roles for the agency's greater good.[12] The Risk and Insurance Management Society (RIMS), and the Institute of Internal Auditors (IIA) conducted such a constructive dialogue with respect to private sector organizations.[13] The resulting RIMS-IIA report articulates a win-win resolution:

> The IIA and RIMS believe that collaboration between the disciplines of internal audit and risk management, can lead to stronger risk practices in meeting stakeholder expectations. The two functions make a powerful team when they collaborate and leverage one another's resources, skill sets and experiences to build risk capabilities within their organizations.[14]

The report cites private sector examples of how such collaboration can work in practice. The RIMS-IIA approach calls for the auditor to rely on:

- ERM work products
- Independent input from senior managers that will allow the auditor to develop its own independent risk assessment

This framework allows the auditor to obtain necessary information and hold the risk management function accountable. This approach also allows the auditor to do its work without chilling communications between business units and the ERM function. The report quotes one company official about the practical results of this collaborative division of labor: "If the responsible risk owner has not taken action on their risks that need addressing, the ERM and internal audit teams inquire why this is the case and highlight the status to senior management and the audit committee as appropriate."[15]

But the public and private sectors tend to operate differently in this regard. In the private sector, many people who work in the internal audit function once worked in operations. They generally have a better sense of operational challenges and risks from this experience. By contrast, in some of the larger IG offices, auditors may never have worked for their "parent" organizations. Their offices are generally not co-located; as a result they will have limited interactions with operational people, except if they are on an audit assignment. This can contribute to a more limited perspective on big-picture organizational risk.

Similarly, in a presentation to the Annual Summit of the Association for Federal Enterprise Risk Management, Inspector General of the U.S. House of Representatives Theresa Grafenstine identified both risk management and internal audit (and by extension, the IG function) as distinct and complementary lines of defense for an organization.[16] The box on the next page presents a list of the three "lines of defense" which is a framework frequently used in the audit community.

12. On constructive dialogue, see, e.g., Thomas H. Stanton, "Constructive Dialogue and ERM: Lessons from the Financial Crisis," chapter 32 of John R. S. Fraser, Betty J. Simkins, and Kristina Narvaez, eds., *Implementing Enterprise Risk Management: Case Studies and Best Practices,* Hoboken, NJ: John Wiley & Sons, Inc., 2015.
13. RIMS and The Institute of Internal Auditors, "Risk Management and Internal Audit: Forging a Collaborative Alliance," 2012
14. Ibid., p. 3.
15. Ibid., p. 9.
16. The Honorable Theresa Grafenstine, Inspector General of the U.S. House of Representatives, "Making Risk Management a Core Element of Organizational Success—Audit's Perspective," presentation to the Sixth Annual Federal Enterprise Risk Summit, September 10, 2014.

Lines of Defense

First Line of Defense
- Management controls
- Internal control measures

Second Line of Defense
- Financial control
- Security
- Risk management
- Quality
- Inspection
- Compliance

Third Line of Defense
- Internal audit

Constructive dialogue between risk officials and inspectors general is needed to develop such a win-win relationship so that the two functions benefit one another without getting in each other's way.

Challenge Five: Educating Agency Staff about ERM

Understanding the Challenge

ERM is a concept that can take time to understand. Some officials seem to go through a period of lack of awareness and then suddenly "get it"; they see the importance of ERM and how to implement it. The need for educating agency staff came through in our interviews. One risk officer indicated that ERM is enormously important. Most federal organizations appreciate risk management as it relates to projects and IT systems, but the appreciation and understanding of ERM remains limited.

At another agency, there is a tendency to focus on risks within specific program offices, and assume that risk managers without deep technical qualifications in a particular area of risk may not provide significant value. For example, there are some who seek to focus discussions of acquisition risk exclusively on the work of acquisition and contracting professionals. An understanding of acquisition is certainly important in identifying sources of acquisition risk. However, it does not follow that acquisition and contracting experience alone can necessarily help an organization determine the best value for its acquisition investments and integrate strategic priorities and collaboration across the enterprise. Thus, enterprise acquisition may not be optimal, even if contracting professionals are doing their jobs well. Acquisition professionals alone cannot ensure a mature and best-value approach to an enterprise acquisition risk management program. Moreover, risk management within an acquisition silo needs to be integrated with risk management elsewhere across the organization to achieve the benefits of ERM and maximize the value of the enterprise's portfolio of products and services.

The establishment of a "risk register" at one agency highlighted a need for better understanding of cross-agency "enterprise" risk management among some senior managers. Risks were scored on a basis of likelihood versus impact. The objective was an effective cross-agency "enterprise" risk register that would not only score risk but also prioritize those risks for treatment. The higher the score, the greater the risk. However, one important functional manager sought to downplay these risks and objected to the scoring as incorrectly interpreting high risk to be equivalent to poor management.

One federal agency's risk leader believes that risk management in the federal government is underappreciated. The Federal Managers Financial Integrity Act of 1982 was important legislation in that it imposed the application of internal controls on federal agencies. Despite this important contribution, OMB Circular A-123, has, over the intervening years, become viewed by many in government as a requirement for financial reporting and compliance, but little more. However, while ensuring the accuracy of financial reports is of obvious importance, so too is an understanding of the risk of not achieving important agency goals. In the focused effort to comply with mandates, too many federal organizations have assumed that such effort alone satisfies its responsibilities to conduct risk management.

Despite the progress that many organizations are making, another risk professional is concerned that there is a growing push within other federal agencies to adopt more "internal audit-like" practices and establish risk organizations that are more focused on internal controls than on proactive risk management practices. This can cloud the distinction between risk and audit organizations and their related roles and missions. He cites as one example, concerns over the independence requirements that some federal regulators are imposing on risk organizations and their boards. These requirements potentially mirror those of board audit committees. As a result, he believes this practice is likely to lead to a narrowing of the role of risk management into that of a compliance or audit function, with a focus on internal controls rather than on true risk management. Despite these concerns, he notes that risk management practices are still evolving and remains optimistic that value-added risk management efforts will prevail in the long run.

One risk professional stated that, rather than a meaningful discussion of risk, how to best manage that risk, and assessment that the targeted level of risk is within the risk appetite of the organization, the government response is too often instead focused on internal controls. Such a narrow view of risk management, the professional stated, never generates the important dialogue and responsibility for balancing performance, cost, and risk.

One interviewee discussed the challenge in terms of the need to articulate a vision and value statement for ERM that would resonate across all levels of the organization. From an organizational change management perspective, such a vision and value statement can be key to gaining the necessary organizational support.

Another interviewee stated that a major challenge any oversight or audit agency in federal government faces today is understanding that compliance is but an element of a broader risk management framework. The current view of many in federal agencies is that oversight and audit functions are all about catching non-compliance with laws, regulations and policies, and with almost no concern about achieving mission objectives. This view of audit and oversight is far too often supported by the auditors and oversight organizations when their reports suggest that all risk should be avoided.

Responding to the Challenge

Again, an agency's top managers will need to promote ERM in a consistent manner throughout an agency. This will take time. One agency COO who does understand ERM reported that she is engaged in a five-year process to change the culture of the agency. The COO is seeking to develop a common understanding of ERM and its value and processes. She is also working to ensure that behavior throughout the agency demonstrates risk awareness rather than a merely compliance orientation. Other interviewees reported similar long-term approaches.

One interviewee has been appointed by the agency head to lead a community of practice on risk management and Enterprise Risk Management. The goal is to both improve the level of maturity of internal risk management, and to get risk management integrated into a standard

way of making decisions across the agency. For example, individuals generally have a sense of the risks that their part of the organization faces, but they have no formal risk register in which those risks are documented, risk treatments are detailed, and progress is formally tracked. Moreover, as risk management is improved through discussion in this community of practice, it is expected that greater consistency and application of best practices will evolve across the agency.

Another interviewee stated that meaningful ERM also requires proper incentives to ensure that risk management is given proper recognition. In this particular organization, 60 percent of each employee's individual incentive plan is tied to risk-related initiatives. Specifically, two-thirds of those incentives are tied to achieving risk management goals, and one third is tied to achieving business continuity goals.

One agency has sought to increase its internal operational risk capabilities and, over a two-year period, saw many improvements, including;

- Establishing a small risk team with executive oversight and support from the COO
- Hiring risk officers in key business units with matrixed reporting to the COO
- Purchasing state-of-the-art risk technology to be rolled out across the agency
- Establishing a risk oversight committee that is beginning to systematically review and proactively manage the top agency-level risks and beginning to tie those risks to the agency budget process

The operational risk manager reports that culture change management and demonstration of the value added have been the most significant challenges. Nevertheless, they have been able to move forward significantly over the two-year period toward a more collaborative approach to risk management.

Another interviewee reported that other officials at the agency initially pushed for a program that was focused on internal controls. The agency risk officer worked with others and led the development of a set of more comprehensive risk management practices.

Challenge Six: Demonstrating the Value of ERM

Understanding the Challenge

Several interviewees expressed concern about the difficulty of demonstrating the value of ERM to agency leaders, managers, and employees. In part, this is because of the inherent nature of risk mitigation: It is difficult to demonstrate the value of a costly incident that never occurs. There are other problems as well. One risk professional observed that, in the federal government, the political leadership of an agency often arrives with little to no understanding of the capacity of the organization to successfully carry out various newly assigned initiatives. This is of course true for any new leadership, whether in the public or private sector. What differs in the public sector, however, is the often much greater pressure to undertake politically driven initiatives without an understanding of the processes or the capacity to deliver on those objectives with manageable risk. In such cases there are nearly always early warning signs.

Another agency's first risk report focused on the top risks across the agency. While valuing the results, senior management was very concerned about release of the information. When initially presented, leadership wanted numbered copies, which were afterwards collected and shredded. Moreover, while the executive sponsor indicated that she supported ERM, there did not seem to be much interest in addressing risks that were not included on the GAO High Risk list. This

lack of concern over risks not listed on this list unfortunately reflects the fact that, too often, leaders do not understand risk management and the organizational value that it brings, and are responding only to external pressures coming from such outside sources as the news media, OMB, Congress, GAO, and others.

One leader has a role in helping to manage risk across a major federal cabinet-level department. In his view, the use of a formal risk management process broadly applied across a large organization is building steam, but still has a long way to go. He sees ERM as a means of making better decisions, and as being particularly necessary to achieve desired outcomes within limited budgets.

Responding to the Challenge

The value of ERM can be seen in the increased quality of decision making. With the increased flow of communication about risk-reward tradeoffs, agency managers will be in an improved position to make decisions that maximize overall stakeholder value. As one experienced risk professional said in an interview, "Whether due to a wakeup call from a recent bad experience, or the proactive action of an insightful leader, ERM can reduce the number of bad decisions resulting from the lack of a process that brings to bear risks, obstacles, and other information to generate constructive dialogue. Without such dialogue, the decision too often comes down to either 'go for it' or 'don't do it.'"

The improved decision-making process can be reflected in any or all of the following:

- Identification and monitoring of risks and risk treatment plans presented at all levels of agency management
- Development of new abilities for management to intervene or otherwise redirect resources if shifting environmental conditions require a change in risk treatment plans
- Significant reduction in the frequency of surprises adversely impacting agency reputation and operations
- Emergence of broad and shared understanding of the agency's risk appetite, and the need to accept a level of risk in decision making consistent with the agency's risk appetite
- Improvement in the organization's ability to allocate resources to manage risk across functional and programmatic areas, thereby increasing agency-wide return on investment
- Improvement in agency-wide appreciation of the need to align functional and programmatic goals with agency strategic goals

Six Steps to Successful Implementation of Enterprise Risk Management in the Federal Government

Based on research for this report, the authors believe that progress is being made to infuse federal agencies with more effective risk management, but as noted in the previous section, challenges remain. The authors' own experiences, supplemented by insights from interviews, suggest several approaches. In the end, as managers of agencies that practice more effective risk management attest, the effort can pay off.

Perhaps the greatest danger for an agency or other organization is that risk management becomes a largely empty gesture of compliance with a set of documented actions rather than a meaningful process that adds value to decisions.

In government it is often the agency head, or perhaps the agency chief operating officer, who plays an essential role in ensuring that risk management actually adds value to agency decisions rather than merely serving as a symbolic compliance function. There are important ways in which the agency head can influence the quality of risk management at an agency. In simplest terms, there are six key steps that need to be taken to implement risk management in a government agency.

Step One: Establish a Risk Governance Framework

The first step is to define key players' roles and responsibilities. This needs to be done both government-wide and within each agency. Many different organizations are now involved to some extent in risk management in government. Based on our research, we believe the following roles are essential in implementing risk management in the federal government and individual agencies can help to foster such a culture:

Government-wide

- **The Office of Management and Budget** should continue to encourage agencies to create cultures and processes that support ERM. OMB should inform budget examiners of the principles of ERM so that, in annual budget reviews, they ask agencies to identify major risks and explain how these are being addressed.
- Working through the **President's Council on Integrity and Efficiency (PCIE),** OMB should work with inspectors general to ensure a common understanding of how risk management offices and IG staffs can work together in a manner that best advances mission achievement, while allowing the IG staff to maintain its required independence. If the agency risk function and agency IG can devise ground rules so that they operate as mutually supportive lines of defense, they can achieve much more than if the IG function were to chill the flow of risk information to decision makers who need it to enhance agency performance and forestall potentially major adverse events.

- **The Government Accountability Office** should:
  - Regularly review best practices in risk management, and ERM in particular, in federal departments and agencies
  - Analyze the risk practices of particular agencies and assess the extent to which agencies are accruing vulnerabilities that their risk management processes have failed to identify and address
  - Examine the quality of decisions that management has made about tradeoffs among performance, cost, and risk that are aimed at maximizing delivered stakeholder value

At the Organizational Level

- **Organization heads and chief operating officers** should:
  - Work to weld their top managers into a management team that thinks in terms of the agency's well-being rather than just in terms of their own parts of the organization
  - Create an organization-wide operating committee, supported by a small risk staff, to regularly identify major risks that could impede achievement of the agency's mission and objectives, prioritize these risks, and help to devise treatment plans to deal with the highest priority risks
  - Encourage a culture of communication in the agency so that all employees feel able to surface concerns for consideration by decision makers
- **Organizational heads should designate an individual to lead the risk initiative.** The head of the organization is best positioned to establish a risk function. In some organizations, this has included the designation of a risk officer and the creation of an enterprise-wide risk council comprised of key executives who meet on a regular basis. This approach helps to ensure that the risk officer has an opportunity to bring information to bear on major decisions. The organization head can ensure that the designated risk individual attends the right meetings and that he or she has access to needed resources and information. The individual designated to lead the risk initiative should focus on the following:
  - Generating appropriate information
  - Facilitating the process of managing major identified risks
- **Organization heads and chief operating officers** should enhance their budget processes so that they consider resources, targeted performance, and risk in an integrated manner. If the agency is subject to budget reductions, it will need to revise agency goals, objectives, and processes to ensure that the cuts do not create vulnerabilities that could arise if it tries to carry on its usual business practices without the resources to support them.
- **Inspectors general and other officials with oversight and audit responsibilities** should meet with the agency's risk managers and determine how best to ensure that the effectiveness of the risk function can be evaluated without chilling the necessary flow of risk-related information to the agency-wide operating committee.

Step Two: Create Conditions for Risk Management to Be Effective

Using a functional approach, different agencies direct risk management to address different issues, often focusing on the major types of risk that they perceive. Federal credit agencies may monitor credit risk or counterparty risk. The Department of Homeland Security (DHS) has decided to focus its department-wide efforts on acquisition and investment risk; other departments and agencies are focusing increasingly on cyber risks. However, increasingly, agencies are adopting an ERM approach.

Whether an agency adopts ERM or merely focuses on specific types of functional risk, the agency head must work to ensure that information flows up and down the hierarchy so that risk-related information can flow to decision makers. To ensure information flows across the agency and, indeed, better manage the agency in general, the agency head should seek to weld heads of major units into a management team. That way, these agency "barons" can come to think of risks and rewards more in terms of the fortunes of the entire agency than merely of their own fiefdoms. This is important so that sub-agency unit heads don't seek to address risks merely by shifting them from their organizations to other parts of the agency. Especially in the context of today's rapid flow of information through the media, reputational risk is an element that ties together the fortunes of virtually everyone in an agency, and especially political appointees and senior career officials, if something major goes wrong.

It is also important to staff the risk function with the right people and tools. Reports from risk managers across government indicate that interpersonal skills, not merely analytical strength, are important attributes for staff of a risk office to possess. To do their jobs well, risk officers need to be trustworthy and trusted by senior officials in the agency. After all, unit heads are making themselves vulnerable by revealing concerns about possible major risks and vulnerabilities for which they are responsible. The risk officer must be able to make these unit heads comfortable about sharing information without fearing that it will come back to them as some form of "gotcha" in a bureaucratic fight. If a risk officer can build that trust, it can reassure the unit head, who may need resources that a risk officer can help to allocate if the vulnerability or risk is to be properly addressed. In the end, the quality of risk officers and their access to information are more important than the size of the office and its budget.

Step Three: Integrate Risk Management into Organizational Decision Processes

To be effective, risk management must actually inform organizational decisions. Integrating risk information into the budgeting and performance management processes allows the agency to allocate limited managerial and funding resources to remediate major risks that might otherwise prevent the agency from accomplishing its mission. Integrating risk management with strategic planning allows decision makers to integrate information about major risks into the agency's planning for achieving goals and objectives. The agency head can also ensure that the risk function is represented at the table at major specialized committees that the agency may establish according to its mission and structure.

Step Four: Protect the Risk Function

It is essential for the organizational head to protect the risk function, especially with respect to major players whose fiefdoms may expose the agency to serious risk. This was a pattern that distinguished firms that successfully navigated the financial crisis from those that went out of business or otherwise failed. For example, Thomas Stanton met with one financial firm's risk officer, who explained that she faced a troubling choice: either she would become a pain in top managers' necks as she repeatedly raised concerns about their decisions, or she would be known as the chief risk officer at a company that blew itself up. She left the company in 2006 with her reputation intact; the company fared less well and failed in 2008.

Step Five: Build Risk Awareness into the Agency's Culture

The organization head has the ability and opportunity, as the saying goes, to set the "tone at the top." This includes establishing a culture in which feedback is heard and respectfully

considered. That does not mean that the person providing the feedback is always correct; rather, the key is to respectfully hear the feedback and, if it seems credible, either to validate or invalidate it.

The organizational head, or chief operating officer, as the case may be, has access to many tools for building risk awareness into the culture. Building cooperation and collaboration into individual performance standards is a good way to encourage staff, and especially senior officials, to accept and listen to feedback about risks. Encouraging constructive dialogue between unit heads and the risk function is another important step. Allocating budget resources to address major risks that a sub-agency unit head identifies also can encourage flow of risk-related information. And there are the more subtle cues, such as locating the office of the chief risk officer near the offices of the agency head and chief operating officer, publicly recognizing the chief risk officer at agency events, and requiring unit heads to explain if a major vulnerability comes to light that the unit head failed to reveal first. The agency head will need to continue to nurture risk awareness as a cultural value so that it remains integral to the way people in the agency carry out their activities.

Step Six: Manage Organizational Change

Moving from traditional risk management conducted in functional and programmatic silos to truly collaborative ERM entails significant organizational change management. This should not be disregarded, nor should its importance be minimized in comparison with the amount of attention that is devoted to the technical implementation of aspects of ERM. A complete set of policies and procedures reflecting best practices in ERM will be of little value if those called upon to execute the policies and procedures resist the required behavioral changes. An organization's culture must support ERM if it is to be effective.

For Further Reading

John Fraser and Betty J. Simkins, *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, Hoboken, NJ: John Wiley & Sons, Inc., 2010.

John R.S. Fraser, Betty J. Simkins, and Kristina Narvaez, *Implementing Enterprise Risk Management: Case Studies and Best Practices*, Hoboken, NJ: John Wiley & Sons, Inc., 2014.

Karen Hardy, *Managing Risk in Government: An Introduction to Enterprise Risk Management* (Second Edition), Washington, D.C.: IBM Center for The Business of Government, 2010.

Young Hoon Kwak and Julia B. Keleher, *Risk Management for Grants Administration: A Case Study of the Department of Education*, Washington, D.C.: IBM Center for The Business of Government, 2014.

Anette Mikes, *Enterprise Risk Management at Hydro One (Multimedia)*, Boston, MA: Harvard Business School, June 2010.

Thomas H. Stanton and Douglas W. Webster, eds., *Managing Risk and Performance: A Guide for Government Decision Makers*, Hoboken, NJ: John Wiley & Sons, Inc., 2014.

Thomas H. Stanton, *Why Some Firms Thrive While Others Fail: Governance and Management Lessons from the Crisis*, New York: Oxford University Press, 2012.

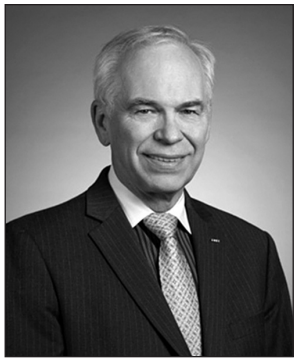
Robert Thames and Douglas W. Webster, *Chasing Change: Building Organizational Capacity in a Turbulent Environment*, Hoboken, NJ: John Wiley & Sons, Inc., 2009

Acknowledgments

In conducting research for this study, the authors interviewed a number of federal executives to gain insights into challenges and suggestions for moving forward. We would like to express our thanks to the following people, as well as the others, who generously contributed to this report:

- Theresa Grafenstine, Inspector General, United States House of Representatives
- Chris Mihm, Managing Director, Strategic Issues, Government Accountability Office
- Steve Smith, Director, Office of Disaster Planning and Enterprise Risk Management, Small Business Administration
- Andy Zino, Senior Advisor to the Under Secretary for Finance & Administration/Chief Financial Officer, Smithsonian Institution

About the Authors



Douglas W. Webster is a Senior Fellow with the George Washington University Center for Excellence in Public Leadership, where he teaches Enterprise Risk Management. He is also the Director of Government to Government Risk Management at the U.S. Agency for International Development and the founder and former president of the Cambio Consulting Group.

In 2011, he co-founded the Association for Federal Enterprise Risk Management (AFERM) and served as AFERM's first president. In 2007 he was confirmed by the U.S. Senate as the Chief Financial Officer of the U.S. Department of Labor, where he served until the end of the George W. Bush administration. In 2004, he served as the Principal Finance Advisor to the Iraq Ministry of Transportation under the DoD Coalition Provisional Authority, Baghdad, Iraq. Dr. Webster served a 21-year career in the U.S. Air Force as a C-130 navigator, including combat in Vietnam, as an air operations officer, and as a senior acquisition and engineering management officer.

Dr. Webster co-edited, with Thomas H. Stanton, *Managing Risk and Performance: A Guide for Government Decision Makers*, (John Wiley & Sons, Inc., 2014). He is also the co-author of two other books: *Activity-Based Costing* and *Performance* and *Chasing Change: Building Organizational Capacity in a Turbulent Environment.*

Dr. Webster serves on the boards of the Pentagon Federal Credit Union and the Penfed Foundation, a charitable organization serving America's veterans and their families. He is a Fellow of the National Academy of Public Administration.

Dr. Webster received a BS in Engineering from the University of California-Los Angeles in 1972, an MS in Systems Management from the University of Southern California in 1983, and a Doctorate in Business Administration from U.S. International University in 1991.

Thomas H. Stanton teaches at Johns Hopkins University. He is President of the Association for Federal Enterprise Risk Management (AFERM) and a former member of the federal Senior Executive Service. He is a Fellow and former board member of the National Academy of Public Administration and formerly chaired the Academy's Standing Panel on Executive Organization and Management. With a career that spans the practical and the academic, Mr. Stanton's work has led to the creation of new federal offices and approaches to delivering public services more effectively.

Mr. Stanton has written several books including *A State of Risk: Will Government Sponsored Enterprises Be the Next Financial Crisis? (*HarperCollins, 1991), in which he invented the concept of contingent capital (see p. 182) now being applied to major financial institutions internationally to help mitigate financial risk. He edited *Meeting the Challenge of 9/11: Blueprints for Effective Government* (M.E. Sharpe Publishers, 2006) and *Making Government Manageable* (co-edited with Benjamin Ginsberg, Johns Hopkins University Press, 2004).

Mr. Stanton's book, *Why Some Firms Thrive While Others Fail: Governance and Management Lessons from the Crisis* (Oxford University Press, 2012), analyzes differences in leadership, governance, and risk management between firms that successfully navigated the financial crisis and those that failed. Mr. Stanton co-edited, with Douglas Webster, *Managing Risk and Performance: A Guide for Government Decision Makers,* (John Wiley & Sons, Inc., 2014).

Mr. Stanton holds degrees from the University of California at Davis, Yale University, and the Harvard Law School.

Key Contact Information

To contact the authors:

Douglas Webster
Sr. Fellow
Center for Excellence in Public Leadership
George Washington University
3100 Hemlock Point Ct
Triangle, VA 22172
(703) 625-7619

e-mail: businessdr@aol.com

Thomas H. Stanton
Fellow
Center for Advanced Governmental Studies
Johns Hopkins University
1717 Massachusetts Avenue, NW, Suite 104
Washington, DC 20036
(202) 965-2200

e-mail: tstan77346@gmail.com

Reports from IBM Center for The Business of Government

For a full listing of IBM Center publications, visit the Center's website at **www.businessofgovernment.org.**

Recent reports available on the website include:

Acquisition

Eight Actions to Improve Defense Acquisition by Jacques S. Gansler and William Lucyshyn
A Guide for Agency Leaders on Federal Acquisition: Major Challenges Facing Government by Trevor L. Brown

Collaborating Across Boundaries

Inter-Organizational Networks: A Review of the Literature to Inform Practice by Janice K. Popp, H. Brinton Milward, Gail MacKean, Ann Casebeer, Ronald Lindstrom
Adapting the Incident Command Model for Knowledge-Based Crises: The Case of the Centers for Disease Control and Prevention by Chris Ansell and Ann Keller

Improving Performance

Balancing Independence and Positive Engagement: How Inspectors General Work with Agencies and Congress by Dr. Charles A. Johnson, Dr. Kathryn E. Newcomer, and Angela Allison
New Jersey's Manage By Data *Program: Changing Culture and Capacity to Improve Outcomes* by David Lambert and Julie Atkins

Innovation

A Guide for Making Innovation Offices Work by Rachel Burstein and Alissa Black
The Persistence of Innovation in Government: A Guide for Innovative Public Servants by Sandford Borins

Leadership

Best Practices for Succession Planning in Federal Government STEMM Positions by Gina Scott Ligon, JoDee Friedly, and Victoria Kennel

Managing Finance

Managing Budgets During Fiscal Stress: Lessons For Local Government Officials by Jeremy M. Goldberg and Max Neiman

Risk

Risk Management for Grants Administration: A Case Study of the Department of Education by Young Hoon Kwak and Julia B. Keleher

Strengthening Cybersecurity

Defining a Framework for Decision Making in Cyberspace by Dighton Fiddner

Using Technology

Using Innovation and Technology to Improve City Services by Sherri R. Greenberg
Participatory Budgeting: Ten Actions to Engage Citizens via Social Media by Victoria Gordon

IBM Center for
The Business of Government

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit: ibm.com

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342
website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.