CHAPTER SEVEN

Assessing Risk

Michael J. Keegan

Highlights

- Since the 1990s, the federal government has substantially expanded its focus on managing risks inherent in its programs and activities.
- Over the past twenty years, agencies have evolved from a focus on compliance-based internal operational control and siloed approaches that address specific kinds of risk—such as financial, security, or program-specific risks—to adopt an organization-wide enterprise risk management approach.
- Enterprise risk assessments are increasingly being incorporated into other government processes, such as strategic planning, resource allocation, decision-making, and internal controls. This trend brings processes together to create an integrated governance structure that will improve mission delivery, reduce costs, and mitigate the range of critical risks facing agencies.

ASSESSING RISK

By Michael J. Keegan

In 2004, the U.S. Department of Education's Office of Federal Student Aid (FSA) established an enterprise risk management organization and hired its first chief risk officer, Stan Dore. Its goal was to strengthen FSA's financial integrity and internal controls. This management decision exemplified the agency's commitment to resolving high-risk organizational issues and emphasized the importance of proactively identifying and managing risks, especially at the strategic or enterprise level. In fact, as FSA began to systematically pursue risk management, in 2005, the Government Accountability Office removed FSA from its list of High-Risk programs.

As the first chief risk officer for FSA, Dore led the effort to develop and prioritize activities for establishing and implementing an Enterprise Risk Management (ERM) vision, strategy, and framework. FSA began to implement an international standards-based ERM approach. Most federal agency efforts relating to risk had been limited to financial and internal control activities. Dore, like other ERM champions in federal agencies, faced a limited availability of ERM guidance, best practices, and other strategic approaches to identify, assess, and manage risk in government.

Despite these challenges, FSA moved forward to establish a foundation for implementing its own ERM program. Fourteen years later, this example and experience serves as a guide for other agencies working to respond to requirements from the Office of Management and Budget (OMB) and to realize the benefits of ERM.

INTRODUCTION

This world is fraught with uncertainty, and all activities entail a certain level of risk. The increasing complexity and interconnectedness of today's society only ups the ante on the unknown. What makes a difference for individuals and organizations alike is how well they can handle an uncertain environment, with risks ranging from financial to reputational to operational. The way to manage this uncertainty is to build government's capacity to anticipate and be resilient – to prepare for the future and its effects.

Government agencies are hardly immune to the effects of uncertainty, such as sequestration, budget cuts, or a government shutdown. Along with these threats, each day federal agency leaders face similar, as well as unique, risks associated with fulfilling their respective program missions. Today's

headlines are full of stories about troubled website launches, cyber hacks, abuses of power, extravagant spending, and a host of other risk management failures. The U.S. federal government has taken a hit, with the public's trust in government continuing to be low as measured in numerous surveys.[1] This view stems in part from stories about how federal agencies could have improved their operational and mission performance, had leaders taken the time to foresee and mitigate potential risks.

Defining Risk as "Uncertainty that Matters"

The first step in tackling risk is defining it. The conventional view of risk focuses on potentially negative effects. Risk management in this context typically addresses managing threats to objectives. As Thomas Stanton and Douglas Webster describe in their 2014 book, *Managing Risks and Performance: A Guide for Government Decision Makers,*[2] defining risk as merely a threat that objectives will not be achieved leaves unanswered the question of how to actively balance risks that may pose opportunities as well as threats.

Maximizing the opportunity for success requires that threats and opportunities are managed together. As government leaders allocate and invest resources and develop strategic plans for their agencies, it is apparent that not all risks are threats -- some in fact bring opportunities. All future events and the achievement of future results—the heart of strategic planning—are uncertain because they have yet to happen. In identifying, analyzing, and mitigating risk, the methods of Enterprise Risk Management (ERM) can also be a powerful resource for strategic planning and effective decision making. To that end, government leaders should view risk as "uncertainty that matters."

When does risk matter? Webster underscores that this occurs when risk has a material impact on the achievement of an agency's strategic objectives and mission execution.[3]

With uncertainties that face government widening and deepening, external and internal risks pose threats to achieving an organization's goals and objectives. Such risks include strategic, cyber, legal, and reputational, as well as a broad range of operational risks such as information security, human capital, financial control, and business continuity. Risks come from both outside and inside an organization:[4]

External risks. Factors as diverse as an aging workforce, changing social norms, or increased cybersecurity threats impact federal agencies in multiple ways. Changes in the external environment produce numerous risks over which the organization has little to no direct control. Having limited control over external risks, however, does not mean ignoring them. Instead, agencies should assess external risks as part of evaluating the impact on achieving their objectives, and the range of options available to address or mitigate that impact.

Internal risks. In addition to risks caused by events outside the organization's control, internal risks can be affected by organizational actions. These actions include internal processes, such as controls, training, values and culture. They are under the direct influence, if not outright control, of the organization.

Risks come in many different dimensions. The box below provides examples of the types of external and internal risks that organizations face, as described in a 2015 report, *Improving Government Decision Making through Enterprise Risk Management,* by Douglas Webster and Thomas Stanton.[5]

Examples of Types of External and Internal Risks

- **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 Barnler, "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.

Ways of Managing Risks

This chapter explores three approaches to managing risks in government:

- **Use of internal control:** The U.S. Government Accountability Office (GAO) has defined "internal control" as a set of activities that provides reasonable assurance that the objectives of an agency will be achieved—specifically, effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.[6]
- **Use of siloed approaches to risk management:** The International Standards Organization (ISO) defines "risk management" as coordinated activities that direct and control an organization with regard to risk.[7] In 2006, GAO defined this as a continuous process of assessing risks, reducing the potential that an adverse event will occur, and putting steps in place

to deal with any event that does occur.[8] Risk management involves a continuous process of managing—through a series of mitigating actions that permeate an entity's activities—the likelihood of an adverse event and its negative impact. Typically, traditional risk management has been implemented in "silos"—that is, specific functions such as financial management, or specific programs such as flood management.

- **Use of Enterprise Risk Management (ERM):** The international risk management society, RIMS™, defines ERM as "a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio," rather than addressing risks only within silos.[9] ERM provides an enterprise-wide, strategically aligned portfolio view of organizational challenges that offers improved insight about how to more effectively prioritize and manage risks to mission delivery.

The first two approaches provide the necessary foundations for the effective use of the third. According to OMB: "ERM is viewed as a part of an overall governance process, and internal controls as an integral part of risk management and ERM."[10]

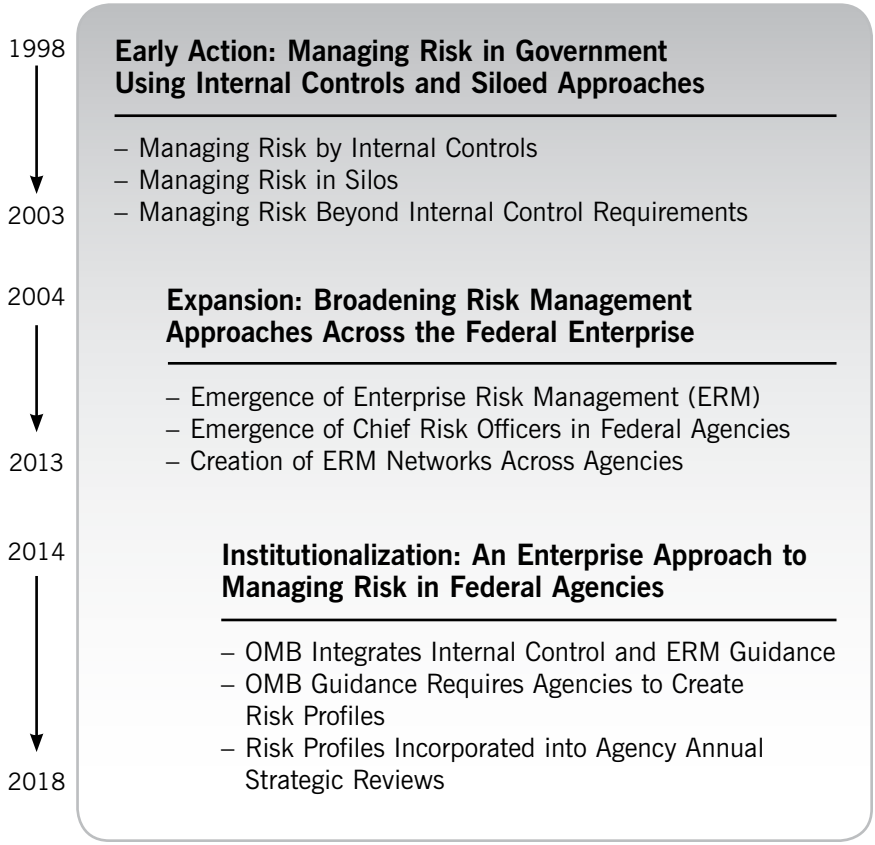
Organization of Chapter

As seen in the chart below, "Evolution of Risk Management: 1998-2018," this chapter describes the evolution of risk management policies in U.S. federal agencies over a twenty-year period. This evolution can be divided into three phases:

- **Early action:** Early efforts in the 1980s and 1990s to manage risk in government focused largely on internal and administrative controls, with some application of traditional risk management principles. Congress passed laws, OMB issued guidance, and the General Accounting Office (since renamed the Government Accountability Office) defined standards—all in an effort to prescribe how federal agencies should manage internal risks (i.e., financial, human resources, systems, compliance, and operations risks). This early emphasis on internal control was part of a burgeoning movement focused on improving accountability in federal programs and operations that addressed fraud, waste, and abuse (see, for example, the box about GAO's High-Risk Government Programs later in this chapter). Federal agencies also began to employ, on an ad hoc and frequently siloed basis, risk management approaches to manage functional risks. Risk management practice also matured generally, with the issuance of a "first of its kind" standard risk management framework and process by the international Committee of Sponsoring Organizations of the Treadway Commission (COSO).

- **Expansion:** Recognizing the benefits of managing risk from an organization-wide enterprise perspective, federal agencies incrementally expanded their use and adoption of formal ERM disciplines and principles beginning in the early 2000s. Lacking a formal federal risk management policy, agencies acted independently to leverage practices with proven track records in the private sector and had access to an increasing number of ERM frameworks and processes. The emergence of chief risk officers began in federal agencies. The coalescing of informal networks of risk management practitioners and thought leaders championed the benefits of ERM as a critical management tool. Revised OMB policy guidance on agency strategic planning and reviews suggested the use of ERM in agency strategic planning, signaling ERM as the way forward for managing risk in federal agencies.

Evolution of Risk Management: 1998—2018



- **Institutionalization:** Technological advances have made federal agency systems, infrastructure, processes, and technologies interconnected and interdependent, such that a risk encountered by one area impacts other operations. This interconnected environment makes the managing of risk across the enterprise more necessary than ever. It also precipitates a change in how government leaders view risk, no longer thinking about risk management as largely a compliance exercise or perceiving risks in solely negative terms as something to be avoided. With that as the backdrop, OMB revised its risk management guidance, Circular A-123, setting forth for the first time a formal governmentwide policy for how government leaders should manage risk and internal control in their agencies. Federal agencies must now implement an ERM framework that also integrates their existing internal control process.

The remainder of this chapter discusses each of these phases, highlighting how federal agencies manage risk, describing the evolution of U.S. federal risk management policies, and offering insights and best practices from IBM Center reports. The chapter concludes with lessons learned and observations of what's on the horizon for federal agencies as they implement and use ERM.

EARLY ACTION: MANAGING RISK IN GOVERNMENT USING INTERNAL CONTROLS AND SILOED APPROACHES

Unlike countries such as Canada and Great Britain, during this period the U.S. lacked a governmentwide risk management policy. Agencies complied with a host of laws and requirements that focused on managing risks associated with a specific functional activity, but no overarching governmentwide policy prescribed an approach to risk management in the federal government. This section explores the building blocks of internal control and the use of siloed approaches to traditional risk management that set the future foundation for what followed—a more strategic use of enterprise risk management.

Managing Risk Using Internal Controls

The early efforts of managing risk in government focused on internal and administrative controls. OMB issued Circular A-123 in 1981, prescribing assessment and reporting requirements for internal financial and administrative controls. Subsequently, Congress passed the Federal Managers Financial Integrity Act of 1982 (FMFIA),[11] an important step in the evolution of federal accounting—and the initial step in taking internal control and risk management seriously. In parallel, GAO developed internal control standards with its

release of *Standards for Internal Control in the Federal Government* (often called the "Green Book").[12] FMFIA and OMB Circular A-123 have remained at the center of federal requirements to improve accountability in federal programs and operations. Eight years later, passage of the Chief Financial Officers Act of 1990 (CFO Act)[13] compelled the development of an infrastructure for auditable financial statements.

These laws, their accompanying guidance, and the financial management framework they built helped federal agencies arrive at a common definition of internal controls and risk management.[14]

What Are Internal Controls?

Internal controls are a set of activities that provide reasonable assurance that the objectives of an agency will be achieved. For example, the organizational objective for financial reporting is to provide financial statements free of material omission or error. Internal controls focus on operational effectiveness and efficiency, reporting, and compliance with applicable laws and regulations—they are a way to manage internal risk. These controls primarily address traditional financial, compliance, transactional, and operational risks, with a focus on risk reduction through the application of discrete controls. Risk assessments traditionally review past performance and activities and are generally not forward-looking. The risks are identified and managed in a siloed, non-integrated basis (e.g., financial reporting, information technology, or physical assets) and documented through external reporting requirements (e.g., audit reports or identified material weaknesses).

Source: U.S. Government Accountability Office, S*tandards for Internal Control in the Federal Government*, 2014 Edition

Managing Risk in Silos

After these earlier requirements were established, additional legislation and regulations soon followed, prompting a renewed focus on internal control and the managing of risk. These efforts—largely by Congress—continued, and on some level reinforced, a siloed approach to risk management:

- **Program risk:** GAO established its High-Risk List in 1990 to call attention to agencies and program areas at high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation (see accompanying box).
- **Performance risk:** The Government Performance and Results Act of 1993 (GPRA) required agencies to clarify their missions, set strategic and annual performance goals, and measure and report on performance toward those goals.[15]

- **Financial management risk:** The Federal Financial Management Improvement Act of 1996 (FFMIA) identified internal control as an integral part of improving financial management systems.[16]
- **Information security risk:** The Federal Information Security Management Act 2002 (FISMA) required each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the agency.[17]
- **Improper payments risk:** The Improper Payments Information Act (IPIA) of 2002 required agencies to annually review their programs and activities to identify those susceptible to significant improper payments.[18]

Almost every one of these legislative mandates required agencies to better manage risk and improve controls in discrete areas. Virtually all of these requirements ultimately focused on a common objective—improved risk management—so that an agency's response to risk provides reasonable assurance that the organization will achieve its strategic objectives. However, these separate requirements were not strategically linked.

To comply with the requirements of each of these new mandates, agencies usually put into place risk management and compliance programs. Karen Hardy's 2010 report, *Managing Risk in Government: An Introduction to Enterprise Risk Management,* says: "This stovepiped approach to compliance is costly and does not optimize value."[19] The dramatic increase in compliance requirements, coupled with the realization that effectively managing risk cannot be achieved simply through discrete risk compliance programs in various business units, has contributed to the movement toward an enterprise-wide risk management approach in the government.

GAO Identifies High-Risk Government Programs

As federal agencies began to focus on internal control, putting the systems and process in place, GAO began identifying high-risk government programs. Since 1990, every two years at the start of a new Congress, GAO calls attention to agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation. The value of this work in terms of highlighting risk management cannot be overstated. It has brought much-needed attention to problems impeding effective government and costing billions of dollars each year.

To help improve these high-risk operations, GAO has made hundreds of recommendations. Executive agencies either have addressed or are addressing many of them and, as a result, progress has been made in a number of these areas. GAO uses five criteria to assess progress in addressing high-risk areas: (1) leadership commitment, (2) agency capacity, (3) an action plan, (4) monitoring efforts, and (5) demonstrated progress.[20]

As Don Kettl points out in his 2016 report, *Managing Risk, Improving Results: Lessons for Improving Government Management from GAO's High-Risk List,* a careful look at the high-risk list reveals useful insights and a roadmap for improving the performance of all government programs. Patterns emerge from the progress that agencies have made in getting off the list. The steps taken to get off the list are the very steps government executives should follow every day. The high-risk list is particularly useful to risk managers, chief risk officers, and agency leadership because it serves as an independent review for flagging risk areas that may be missed by agencies.[21]

Managing Risk Beyond Internal Control Requirements

As Karen Hardy chronicles in her 2015 book, *Enterprise Risk Management: A Guide for Government Professionals,* despite federal agency compliance with a wide range of statutorily required reporting requirements over the years, a volatile environment involving fraud in the financial industry "prompted a reexamination of the existing internal control requirements for federal agencies."[22]

After the passage of the private-sector-oriented Sarbanes-Oxley Act of 2002 to strengthen corporate financial reporting, OMB revised Circular A-123 in 2004 in order to strengthen internal control over internal federal financial reporting. OMB also emphasized the need for agencies to integrate and coordinate these controls with other internal control-related activities. The latter objective, according to Hardy, represented a critical shift that expanded the view of risk in the evaluation of internal controls. This shift was just one small step towards the use of ERM in government.

Risk management and internal control as implemented in the 1990s were important aspects of an organization's governance, management, and operations. However, as Hardy notes, "internal control guarantees neither the success of agency programs nor the absence of waste, fraud, and mismanagement, but is a means of managing the risk associated with federal programs and operations."[23] This is why the early phase begins with a focus on the establishment of internal control policy within the federal government; federal agencies first managed specific types of risks, like those having to do with internal systems and process that could compromise an agency's ability to operate. Starting with how federal agencies manage internal risks via internal control led to key policy and guidance documents such as Circular A-123 and GAO's *Standards for Internal Control in the Federal Government.* Throughout the years, the revisions and updates to these documents chronicle the evolving approach to managing risk in government. In fact, both documents played a role in how the federal government has moved towards adopting ERM.

While federal agencies complied with the requirements surrounding internal control, pockets of activity appeared within the government applying risk

management principles to address and manage programmatic challenges. For example, the Department of Labor applied traditional risk management approaches to reduce its level of improper payments.

Department of Labor: Using Risk Management to Reduce Improper Payments

In a 2016 report, *Risk Management and Reducing Improper Payments: A Case Study of the U.S. Department of Labor*,[24] Robert Greer and Justin Bullock provide a case study on how the department developed and implemented risk management strategies to reduce improper payments in the Unemployment Insurance program. Unemployment Insurance is a jointly administered federal-state program that provides benefits to eligible workers unemployed through no fault of their own. This program is a federal-state partnership based on federal law, but administered by state government employees under state law.

In 2010, Congress passed the Improper Payment Elimination and Recovery Act. This statute set a 10 percent improper payment rate as a limit for federal programs. The improper payment rate for Unemployment Insurance had fallen from 2006 to 2009, but began to increase in 2010 and remained in violation of the statute's standard for improper payments.

Improper payments are a type of operational risk. In response, the Department of Labor implemented eight risk management strategies to combat improper payments, thereby minimizing financial and reputation risks to the program. One of the eight strategies was to increase collaboration between the states and the federal government to aid states in lowering improper payments across all of the program's elements.[25]

Limitations to Managing Risks in Silos

The early action phase was characterized by the use of internal controls and siloed approaches to manage risk in government. These efforts served two useful purposes:

- Internal controls focused on internal risks that can compromise the operation of an agency—effectiveness and efficiency, financial accountability, and the ability to comply with all laws and regulations.
- The functional- and program-based siloed risk management approaches in specific areas, such as improper payments, performance, and cyber, helped develop risk management capabilities in pockets around the government.

However, the "[most significant] limitations in traditional risk management practice," note Thomas Stanton and Doug Webster, "is the treating of

risks within functional and programmatic silos."[26] This siloed approach to risk management lacked a central point of coordination and provided no basis for ensuring a consistent approach to risk management. In addition, no single organization or person focused on ensuring the development of an integrated view of risks (across all functional or organizational silos) that aligns with an overall enterprise strategy.

The 2015 report, *Improving Government Decision Making through Enterprise Risk Management,* by Doug Webster and Thomas Stanton, details key limitations to the siloed approach to managing risk, including:

- Gaps in the identification, assessment, and treatment of risks between functions, programs, or organizational subdivisions
- Inefficiencies due to overlaps in the treatment of shared risk
- Inconsistencies in the treatment of risks by various functions due to dissimilar risk appetites and approaches to risk management
- Lack of strategic alignment
- Reduced return on investment in the application of limited resources to the delivery of a portfolio of products and services[27]

EXPANSION: BROADENING RISK MANAGEMENT APPROACHES ACROSS THE FEDERAL ENTERPRISE

Recognizing the benefits of managing risk from an enterprise perspective, agencies expanded the use and adoption of the formal discipline of ERM and its principles. As Webster and Stanton note, "Despite the initially slow progress and misunderstanding of the term ERM, concrete progress is now demonstrably underway."[28] This expansion phase describes progress in key aspects of ERM. The discussion below highlights examples of its expanded use among federal agencies, identifies selected benefits and challenges of ERM, and presages the trends toward institutionalization.

What Is Enterprise Risk Management?

The Association for Federal Enterprise Risk Managers (AFERM) defines 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."[29] This definition provides leaders a forward-looking view of risk that can better inform strategy and business decisions. It allows for more risk management options through enterprise-level tradeoffs, versus a primary focus on reducing risk through controls. It explicitly addresses risk appetite and tolerance. Effective ERM facilitates improved deci-

sion making through a structured understanding of opportunities and threats.

Webster and Stanton sum it up succinctly in their 2015 report: "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,' which 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 programmatic silos."[30] They also note that the need to incorporate risk management into the strategic planning process is an inherent part of any meaningful ERM program, which again requires a comprehensive view of major risks to the agency and its programs.

Examples of Federal Agencies Using Enterprise Risk Management

Implementing an ERM program takes hard work, and often the push to implement comes on the heels of a risk-related failure. The following two examples illustrate the efforts and experiences of pioneering federal agencies that implemented ERM in advance of any failures.

Office of Federal Student Aid: An Early Pioneer in the Use of ERM

The U.S. Department of Education's Office of Federal Student Aid (FSA) put in place the first formalized ERM framework in the federal government, starting in 2004. Some 14 years later, this example and experience serve as a guide for other agencies working to realize the benefits of ERM.

FSA works to ensure that all eligible individuals can benefit from federal financial assistance for education beyond high school.[31] Over time FSA has granted or guaranteed more than $1.2 trillion in student loans, with 40 million borrowers at more than 6,000 universities around the country. Given the size of its loan portfolio, coupled with a high student loan default rate at the time, GAO placed FSA on its High-Risk List of programs in 1990. In 1998, FSA was legislatively designated as a "performance based organization" which allowed it a certain degree of autonomy, and its chief operating officer was appointed by the Secretary of Education on a term contract. Some have noted that being designated a performance-based organization "helped pave the way" for the creation of a risk management function at FSA.[32]

The department's goal of strengthening financial integrity and internal controls was the primary driver behind FSA's decision to establish an ERM organization and hire FSA's first chief risk officer (CRO), Stan Dore.[33] This management decision exemplified the agency's commitment to resolving potentially high-risk organizational issues and emphasized the importance of proactively identifying and managing risks, especially at the strategic or enterprise level. As FSA began to systematically pursue risk management in 2004, the following year GAO removed FSA from its High-Risk list. As the first CRO, Dore led the effort to develop and prioritize activities for establish-

ing and implementing an ERM vision, strategy and framework at FSA. He set out to create an enterprise-wide risk management office, which formally stood up in 2006.

FSA began to implement a COSO-based ERM framework (see box below for a discussion of the COSO framework). Since most federal agency efforts relating to risk had focused primarily on financial controls, Dore had limited ERM guidance, best practices, or other strategic approaches for identifying, assessing and managing risk. Despite these challenges, FSA moved forward with establishing a foundation for implementing its own ERM program.[34] In 2007, the then-chief operating officer and sponsor for the risk management office left FSA. FSA had several acting leaders until a full-time chief operating officer was named in 2009. The new chief operating officer, Bill Taggart, was a former bank executive and a strong supporter of risk management. He appointed a new chief risk officer, Fred Anderson, who raised the profile of the office, expanded the risk management framework, and formalized the role of risk management in FSA's five-year strategic plan.

In addition, Anderson chaired a cross-FSA Risk Management Committee, which includes FSA operational and business leaders. The committee met monthly and Taggart attended all meetings. The committee was "intended to assess and evaluate major strategic risks, establish the organization's risk profile, and set risk tolerances [across the organization]."[35]

Defense Logistics Agency: Top Leadership Support is Key

A key lesson in implementing an ERM program is the importance of top leadership support. In 2009, the then-director of the Defense Logistics Agency (DLA), Vice Admiral Alan Thompson, developed his strategic priorities for the agency, including introducing ERM into the agency.

DLA is the nation's combat logistics support agency that manages the global supply chain—from raw materials to end users to disposition—for the Army, Navy, Air Force, Marine Corps, Coast Guard, 10 combatant commands, and other federal agencies. At the time, VADM Thompson led a global enterprise with operations in 48 states and 28 countries, and fiscal year 2009 sales and services of close to $38 billion, which would place it in the top 65 on the Fortune 500 list of companies.[36]

VADM Thompson identified three key priority areas that framed his strategic direction for DLA: warfighter support, stewardship excellence, and workforce development. The second-priority area involves enhancing the DLA's stewardship of resources, for which managing risk at DLA took on an enterprise approach. In 2009, Thompson established its ERM function, with the goal of bringing together existing risk management activities and strengthening its Stewardship Excellence initiative.[37]

Prior to establishing its ERM function, DLA instituted risk-based pilot programs. These programs showed that one organizational component would

sometimes identify a potential risk that another component had already experienced and resolved.[38] ERM seemed like the right solution to reduce this siloed and fragmented approach to risk management. Once implemented, DLA focused on developing a standardized, repeatable process for identifying and assessing risks, making recommendations to leadership for actions on those risks, tracking the actions taken in response, and learning from the process, to make DLA more efficient and effective.[39]

Under the leadership of VADM Thompson, DLA recognized that success would come from embedding a consistent set of risk management principles, concepts, and shared language across the agency. It established a small ERM staff office headed by chief risk officer. To leverage the inherently collaborative nature of other successful ERM programs, DLA established a broad-based ERM community of practice—encouraging robust discussion among a multifunctional management group, to arrive at an enterprise view of risks in the agency.

Expanding the Use of Risk Management Frameworks and Processes

As the use of ERM expanded, so did the use of recognized ERM frameworks, such as the international COSO and ISO 31000 standards, to guide the success of the expansion. The federal agencies profiled above adopted the COSO ERM framework to guide their implementation efforts.

Another use for ERM involved the managing of specific risks related to IT systems and cybersecurity. During this period, the National Institute of

Risk Management Framework Standards

Risk management frameworks provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization.[40] The following two international organizations have established widely used standards:

Committee of Sponsoring Organizations of the Treadway Commission (COSO). Originally issued in 2004, COSO's *Enterprise Risk Management—Integrated Framework,* expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. It was updated and re-titled in 2017 to *Enterprise Risk Management–Integrating with Strategy and Performance.* It expanded its emphasis on risk in both the strategy-setting process and in driving performance.

ISO 31000: 2009/2018 Risk Management—Principles and Guidelines. First released in 2009 and later updated in 2018, this international standard put greater emphasis on the iterative nature of risk management, principles of risk management, and the integration of risk management into governance of the organization.

Standards and Technology (NIST) released *The Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST 800-37,[41] a risk management framework focused on managing risks associated with the federal information systems. This IT risk framework promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust and continuous monitoring processes.

In 2013, Executive Order 13636 called for the creation of a Cybersecurity Framework, a voluntary risk-based strategy—a set of industry standards and best practices to help organizations manage cybersecurity risks. In addition to helping organizations manage and reduce risks, the Cybersecurity Framework fostered risk and cybersecurity management communications among both internal and external organizational stakeholders. In May 2017, Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* required that all federal agencies adopt the Cybersecurity Framework. As of July 2018, an update to this risk management framework was in draft. This update adds an overarching concern for individuals' privacy, helping to ensure that organizations can better identify and respond to these risks, including those associated with using individuals' personally identifiable information.

Applying ERM to Cybersecurity[42]

As government organizations expand operations to include the use of technologies such as social media, the Internet of Things, mobile, and cloud, they inherently extend their cyber exposure. Today more than ever, agencies face an increasing number of cybersecurity risks and threats of data breaches. Cyber risk persists anywhere data exists. This creates a need for cybersecurity risk strategies to protect and manage private and sensitive information.

Government systems continue to have vulnerabilities and to be targets of successful attacks. Examples include the Office of Personnel Management (OPM) and the IRS, as well as Pentagon intrusions and data breaches compromising private information and data. Today's attackers have expanded their reach to not only include anything connected to the internet, but to also work through unaware intermediaries to launch their attacks.

To address these issues, existing ERM plans are expanding to include cyber risk assessment frameworks. The World Economic Forum's *Partnering for Cyber Resilience* report indicates that cyber risk is increasingly viewed as a key component in ERM frameworks. The report quantified cyber risk in a three-fold approach to make sound investment and risk mitigation decisions:

- Understand the key cyber risk drivers required for modeling cyber risks
- Understand the dependences among these risk drivers that can be embedded in a quantification model

- Identify ways to incorporate cyber risk quantification into ERM

ERM has become an integral element in organizational strategy today, and securing data and managing cyber risk must now be viewed as a key component within an organization's ERM framework. Strong IT governance coupled with a rigorous ERM approach is critical to restoring confidence in the security and privacy protections provided by the federal government.

Note: For more insights on properly addressing cybersecurity and privacy risks, please see Dan Chenok's series of blogs on the IBM Center website: http://www.businessofgovernment.org/node/2073

Emergence of Chief Risk Officers in Federal Agencies

Though not mandated, chief risk officers (CRO) continued to emerge in federal agencies. Each agency profiled above established the CRO role. In these and similar cases, CROs champion agency-wide efforts to manage risk within the agency and advise senior leaders on the strategically-aligned portfolio view of risks at the agency. They also serve as strategic advisors to an agency's chief operating officer, as well as other staff, on the integration of risk management practices into day-to-day business operations and decision making. For example:

- The Transportation Security Administration's (TSA) CRO serves as the principal advisor on all risks that could affect TSA's ability to perform its mission, reporting directly to the TSA Administrator.[43]
- The Defense Logistics Agency defined the role of its CRO as akin to an orchestra conductor leading a multifunctional, multitalented, and multiperspective ensemble through a risk management score.[44]
- Though originally established in 2004, the Federal Student Aid CRO did not become a part of the executive team until after 2009. At that time FSA's chief risk officer began to connect the dots across all key business and risk oversight activities of FSA.

A 2014 revision to OMB Circular A-11, *Preparation, Submission and Execution of the Budget,* includes the first mention of the value of the ERM approach (addressed further in the next section). It also provides a valuable description of what an effective enterprise risk manager does:

- Develops, manages, coordinates, and oversees a system that identifies, prioritizes, monitors, and communicates an organization's enterprise-wide risks
- Establishes and provides oversight of policies that enable consistent use of enterprise risk management; ensures the incorporation and dissemination of enterprise-wide risk management protocols and best practices
- Establishes the procedures for determining the amount of risk an agency will accept or mitigate[45]

Creation of ERM Networks and Policy

As federal agencies began to steadily adopt the ERM approach on an ad hoc basis, an informal network of risk practitioners within government self-organized into a Federal Executive Steering Group for Enterprise Risk Management dedicated to expanding the use of ERM. This small but growing network of interested professionals worked to champion the benefits of approaching risk management at an enterprise level. In 2011, this informal network established a formal organization, the Association of Federal Enterprise Risk Management (AFERM). As the only organization focusing on the advancement of risk management principles and standards in the federal sector, AFERM is dedicated to instructing, training, and informing government managers in the field of ERM.

The work of both informal and formal networks has contributed to expanding the use of ERM in agencies, and subsequently the move to institutionalize ERM across the federal government.[46] GAO's Chris Mihm observed: "In a relatively short amount of time, enormous progress has been made in the area of risk management in government. Due to major efforts of many risk managers in the public and private sectors, risk management both as a discipline and a way of thinking has deepened and expanded significantly."[47] He called on the community to continue to expand the discipline across programs, help managers understand and calculate the risk in the status quo, and find ways to use risk management to help address governance challenges.

During the expansion phase, OMB broadened the scope of its existing risk management policy for federal agencies. This broadening, as envisioned at the time, would include the development of guidelines addressing both agency strategic risk management and governmentwide governance of risk management. In 2014, Dave Mader, then controller at OMB, acknowledged that the federal financial community was beginning to think about risk more broadly than just financial risk: "What we are doing 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."[48] At that time, Mader hinted at a flexible approach, not a one-size-fits-all ERM framework.

Identifying Challenges to Institutionalization

Using ERM approaches brings important benefits, but implementing ERM is an iterative process. These benefits cannot be achieved without overcoming specific implementation challenges, such as:

- Providing the appropriate foundation, assessment, and management platform
- Sustaining support from the top

- Positioning ERM as a strategic management practice and not as an additional task
- Addressing power concentrated in silos
- Making trade-offs between competing priorities—key ERM staff participate in various special projects and initiatives that are risk-related, but do not directly support the implementation of an ERM program
- Balancing federal government regulations and requirements
- Overcoming a lack of understanding about risk management and a culture of caution
- Overcoming a lack of qualified risk management professionals and expertise
- Educating agency staff about ERM[49]

INSTITUTIONALIZATION: AN ENTERPRISE APPROACH TO MANAGING RISK IN FEDERAL AGENCIES

Technological advances have made federal agency systems, infrastructure, processes, and technologies so interconnected, and so interdependent, that a risk encountered in one area increasingly has the potential to affect operations in other areas. This interconnected environment also requires a change of mindset for how government leaders view risk, no longer thinking about risk management as a largely compliance exercise or perceiving risks solely as problems to be avoided. It is about reconceiving risk management as a value-creating activity integral to strategic planning and decision making.

OMB Circular A-11 Signals the Way Forward for an Enterprise Approach

As noted earlier, OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget,*[50] provides guidance to agencies on preparing and submitting their budget requests for the upcoming year, and instructions on budget execution for the current fiscal year.

In 2014, OMB revised this circular to encourage agencies to institute an ERM approach and leverage such efforts when conducting their annual strategic reviews. Since agency strategic plans focus on long-term objectives, agencies were to incorporate risks and how risks change over time. Considering risk management in the early stages of the strategic planning process can ensure that the agency's management of risk is appropriately aligned with the organization's overall mission, objectives, and priorities. This signaled to agencies that ERM is a valuable management tool in their strategic planning process. Such an approach, found one former federal chief financial officer,

"can drive strategy, help with performance and drive budget decisions…If you know the risks, then you can make decisions on how to accept, eliminate, or manage them."[51]

OMB Circular A-123 Requires an Enterprise Approach to Managing Risk

In July 2016, OMB updated Circular No. A-123, retitling it from *Management's Responsibility for Internal Controls,* to *Management's Responsibility for Enterprise Risk Management and Internal Controls.* As the new title indicates, the revised Circular makes two significant policy changes:

- It requires federal agencies to use the ERM approach to manage risks.
- It updates policies on internal control, directing federal agencies to follow the latest standards as detailed in GAO's 2014 edition of its *Standards for Internal Control in the Federal Government.*

Ultimately, the revised Circular incorporates ERM as a part of the overall federal governance process, including internal controls as an integral part.[52]

OMB Circular A-123 is the primary guidance to agencies on risk management. Historically, the Circular focused on traditional risk management approaches—the use of internal control systems and compliance with various statutory requirements. Its revision mandates the use of enterprise-wide approaches to managing risk, citing ERM as a discipline that deals with identifying, assessing, and managing risks. The policy states that ERM is an effective agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. This provides an enterprise-wide, strategically aligned portfolio view of organizational challenges, and improves insight about how to most effectively prioritize resource allocations to ensure successful mission delivery.[53]

According to the revised Circular A-123, risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats, and identify previously unknown opportunities to improve efficiency and effectiveness. Agency management is responsible for establishing and maintaining internal controls to achieve specific objectives related to operations, reporting, and compliance. Agencies must consistently apply these internal control standards to meet the principles and related components outlined in the Circular, and to assess and report on internal control effectiveness at least annually.

Agencies must also develop a risk profile, a prioritized portfolio of the most significant risks identified and assessed through the risk assessment process, with priorities based on the likely impact of an identified risk on strategic and operational objectives and coordinated with annual strategic reviews. Circular A-123 complements Circular A-11 by integrating agency responsibilities for identifying and managing strategic and programmatic risk

as part of agency strategic planning, performance management, and performance reporting practices. Taken together, these two circulars now constitute the ERM policy framework for the federal government.

The revised Circular A-123 also prescribes ERM development and implementation deadlines. OMB acknowledges that federal agencies are at different maturity levels in terms of their capacity to fully implement ERM. It calls on agencies to use an iterative approach to refine and improve their efforts at developing risk profiles and implementing ERM each year.[54] In support of this iterative approach, federal agencies have access to resources and tools that can assist them meet the requirements of Circular A-123 and implement ERM, such as:

- The Chief Financial Officers Council's *Playbook: Enterprise Risk Management for the U.S. Federal Government* identifies the objectives of a strong ERM process, laying out seven steps to setting up an ERM model, the so-called "pitfalls" of its implementation, how to determine an agency's risk "appetite" (the level of risk acceptable for an agency to achieve its objective), questions agencies should consider in establishing or reviewing their approaches to ERM, and examples of best practices.[55]
- The Government Accountability Office's *Good Practices in Managing Risk* identified six practices that illustrate ERM's essential elements. The selected good practices represent steps that federal agencies can take to initiate and sustain an effective ERM process, and can apply to more advanced agencies as their ERM processes mature.[56]

Integrating Internal Control and ERM Guidance

As noted earlier, the Federal Managers Financial Integrity Act of 1982 (FMFIA) requires OMB, in consultation with GAO, to establish guidelines for agencies to evaluate their systems of internal control and determine FMFIA compliance. OMB Circular No. A-123 now includes guidance for federal agencies to integrate and coordinate risk management and internal control efforts across the enterprise and between management silos, consistent with the principles for effective internal control in GAO's 2014 edition of its *Standards of Internal Control in the Federal Government.* Internal control can no longer be considered an isolated management tool.

The revised Circular A-123 also requires agencies to establish and maintain internal control to achieve specific objectives related to:

- operations, reporting, and compliance
- assessing and reporting effectiveness
- providing assurances on financial and performance reports that include information regarding identified material weaknesses and corrective actions

Agencies were also directed to develop risk profiles to document their assessments and ensure an appropriate balance between the strength of controls and the relative risk faced by programs and operations. Ultimately, the benefits of controls should outweigh the cost. This shift in policy changes the way government manages risk. To implement these requirements successfully, agencies must incorporate risk awareness into their institutional culture and ways of doing business.

Reflecting Risk in Agencies' 2018 Strategic Review Guidance

In 2018, the Trump administration continued the focus on managing risk more effectively with the issuance of OMB guidance to agencies for conducting annual strategic reviews in accordance to requirements of the GPRA Modernization Act.[57] The 2018 Strategic Reviews built on previous efforts, inclusive of an agency risk assessment that outline significant risks, identified through the development of agency risk profiles, that can impact the achievement of strategic and performance goals.

LESSONS LEARNED

Managing risk in any sector comes with its own unique challenges. Perhaps the greatest challenge for any organization is ensuring that managing risk is a meaningful process that adds value to decisions. Following are some key lessons learned, based on IBM Center reports, research, and experience over the past two decades.[58]

- **First, senior leadership is key.** Effective enterprise risk management begins with establishing the tone at the top of an agency. As illustrated by the Federal Student Aid and Defense Logistics Agency experiences described earlier in this chapter, top leadership support is key in pushing the successful implementation of ERM. Without senior leadership support, getting the necessary buy-in throughout the organization will be unlikely and an ERM effort may be reduced to just another compliance exercise that is not integral to the agency's strategic management discipline. In addition, ERM can improve agency decision making by strengthening both the quantity and quality of the information available, and offering the opportunity for a fact-based information flow that can challenge the leadership team's assumptions.
- **Second, cultivating a risk-aware culture matters.** Agency leadership benefits from embedding systematic risk management into business processes, including strategic planning, policy development, program delivery, and decision making. Doing so goes a long way to developing a positive risk culture that promotes an open and proactive approach

that considers threats and opportunities. In turn, this enables effectively communicating and consulting about risk with relevant stakeholders and facilitates transparent, complete, and timely flows of information between decision makers. Building cooperation and collaboration into individual performance standards encourages staff to accept and listen to feedback about risks. Agency leadership needs to nurture risk awareness as a cultural value so that it remains integral to the way people in the agency carry out their activities.

- **Third, recognize that ERM is an iterative process.** Successful ERM is dynamic, iterative, and responsive to change. Its effectiveness depends on maturity, and agency levels of risk management maturity vary. A critical first step is to define key players' roles and responsibilities, while also creating an organization-wide committee to identify, prioritize, and plan to deal with high-priority risks. Governance frameworks are a critical start, but as the agency processes mature, their governance approach will be refined with each subsequent stage informing the preceding one. For example, FSA developed a time-bound, phased plan for implementing its enterprise risk management approach; each phase had defined risk criteria and an accountable owner, who also was responsible for continuous review and updating based on changing conditions. An upfront investment in planning and engaging senior leaders made the eventual implementation easier to act upon. Such an approach lends itself to reviewing and continuously improving the management of risk so it is not a "one-off event," but rather a process of continuous improvement based on internal reviews.
- **Fourth, enhancing data for decision-making processes are a key contribution of ERM.** The ERM discipline can enhance an agency's existing decision-making processes. ERM starts with a focus on events that could potentially happen and their classification into opportunities and risks. Keeping track of these possible events requires good data and data governance, managed at the enterprise level. Improved data management allows the enterprise to take advantage of modern analytical methods in order to quantify the impact of risks. Data analysis also enables the enterprise to gain an overall view of current risks, as well as trends and potential future risks. An accurate, useful ERM process is based on sound analytics. Both the Federal Student Aid and Defense Logistics Agency examples illustrate that implementing ERM yields benefits to an organization in managing risks and informing its decision making.
- **Fifth, managing change and learning are crucial in shifting to an ERM-based discipline.** Moving from traditional risk management, conducted in functional and programmatic silos, to truly collaborative ERM requires significant organizational change management. A complete set of policies and procedures reflecting best practices in ERM will have little value if those called upon to execute the policies and procedures resist the required changes. An effective organization needs to support ERM. To

that end, agencies should not work in a vacuum, but can learn from the experience of similar operational functions or missions and benchmark risk management practices using data from ERM-focused organizations. A knowledgeable workforce is the key to successful ERM implementation, so a key lesson learned is to hire and train staff with the right skills.

LOOKING FORWARD

The risks facing government agencies are hardly static. They morph and transform in ways never seen before. It is a leadership imperative for government executives to mitigate the potency of uncertainty by managing the realities of risk. In an increasingly uncertain, complex, and interconnected world, the need for determined and adept risk leaders will be greater than ever.

Many current transformations (i.e., blockchain, artificial intelligence, robotics, and smart technologies) have the potential to make government function more effectively. Each of these advances bring unique risks, as well as their potential application in managing current risks. It is a positive change that OMB has mandated the use of ERM, that an increasing number of federal agencies have recognized the value of ERM, and that they are taking actions to make ERM an important part of their operational model to address emerging transformations beyond simply meeting external requirements.

However, today's digitally disruptive environment continues to usher in new and evolving threats. The immediate future is already taking shape:

- **Increased technological risk.** Technological advances—as represented by artificial intelligence, big data, robotics, the Internet of Things, blockchain technology, and the implications of the share economy—are transforming the risk environment and ushering in new benefits and new risk for government. Though the immediate effects of these changes may appear over time, some if not all will permeate the operations of agencies into the future. As one observer notes, "Technological risk is expected to become increasingly complex with the growth of new technologies beyond those currently recognized."[59]

  Given this reality, agency risk architecture and ERM governance will need to identify suitable ways to prioritize, respond, and ultimately manage new and potentially unknown and unknowable risks. Technological risk leads to greater uncertainty, compelling government leaders to look ahead with strategic foresight. Making strategic foresight an integral discipline within ERM can help agencies anticipate risks and prioritize resources accordingly.
- **Increased interconnectedness of different kinds of risks.** Many federal agencies now collaborate with external parties to achieve mission outcomes. This interconnectedness means these entities share data, systems, and thus a level of risk. Agency leaders must identify innovative

ways to manage risk collectively in an increasingly networked and collaborative world. Couple the changing nature of how work is done with the proliferation of new technologies described above, and agency leaders must proactively address the risks associated within an increasingly complex organizational ecosystem.

- **Cultivating agile and adaptive risk leaders.** The perception of risk has evolved over time. Risk is no longer viewed as inherently negative, something to avoid, but as a potential way to create value and enhance performance. Managing risk must become an integral part of an agency's strategic mission. ERM elevates the role of the risk professional from an operational to a strategic level. As a result, risk professionals will need to expand their knowledge and experience while honing essential risk management skills. For example, today's risk leader may have a basic, albeit insufficient, understanding of the components of technological risks. To be ready for the future will require them to become cognizant of technological advances and their implications on how an agency operates. Successful risk leaders in the future must be adaptive, informed, and ready for the impact of inevitable change.

As government operates in a world of increasing speed and complexity, and as citizens expect better, faster, and more cost-effective results, managing risk becomes ever more critical. Government executives need to understand and apply tools and techniques like ERM to their specific operating environment addressing the inherent risks facing the public sector. The promise of ERM, now and into the future, goes to the core of program delivery and mission success.

Michael J. Keegan *is the Leadership Fellow at the IBM Center for The Business of Government and Host of The Business of Government Hour. He has interviewed and profiled hundreds of senior government executives and thought leaders who are tackling some of the most significant public management challenges facing government today. He has more than two decades of experience in both the private and public sectors, encompassing strategic planning, business process redesign, strategic communications and marketing, performance management, change management, executive and team coaching, and risk-financing.*

Endnotes

1 "Government Gets Lower Ratings for Handling Health Care, Environment, Disaster Response," Pew Research Center, December 14, 2017.

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

3 Michael J. Keegan, "Introduction: Pursuing Risk Management in Government—A Leadership Imperative," *The Business of Government Magazine* (Fall 2015): 57, IBM Center for The Business of Government.

4 Daniel J. Chenok, Haynes Cooney, John M. Kamensky, Michael J. Keegan, and Darcie Piechowski, *Seven Drivers Transforming Government,* IBM Center for The Business of Government, 2017, 21.

5 Douglas Webster and Thomas Stanton, *Improving Government Decision Making through Enterprise Risk Management,* IBM Center for The Business of Government, 2015, 6.

6 This definition was first published in GAO/AIMD-00-21.3.1, *Standards for Internal Control in the Federal Government,* November 1999, 4, and slightly updated in GAO-14-704G, 5.

7 International Standards Organization, "ISO 31000:2018 Risk Management – Guidelines," 2018, accessed June 22, 2018, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

8 U.S. Government Accountability Office, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure,* GAO-06-91 (Washington, DC, 2005): 17.

9 "What is ERM?," RIMS, accessed June 6, 2018, accessed June 22, 2018, https://www.rims.org/resources/ERM/Pages/WhatisERM.aspx.

10 Office of Management and Budget, OMB Circular No. A-123: *Management's Responsibility for Enterprise Risk Management and Internal Control,* July 15, 2016, 7.

11 *Federal Managers Financial Integrity Act of 1982,* Public Law 97-255, 1982.

12 U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, DC, 2014).

13 *Chief Financial Officers Act of 1990,* Public Law 101–576, 1990.

14 William R. Phillips, et al., *Public Dollars Transformation: Common Sense for 21st Century Financial Managers,* IBM Corporation, 2003.

15 *Government Performance and Results Act of 1993,* Public Law 103-62, 1993.

16 *Federal Financial Management Improvement Act of 1996,* Public Law 104-208, 1996.

17 *Federal Information Security Management Act of 2002,* Public Law 107-347 Title III, 2002.

18 *Improper Payments Information Act of 2002,* Public Law 107-300, 2002.

19 Karen Hardy, *Managing Risk in Government: An Introduction to Enterprise Risk Management,* IBM Center for The Business of Government, 2010, 5.

20 Karen Hardy, *Enterprise Risk Management: A Guide for Government Professionals* (Hoboken: John Wiley & Son, 2015): 10.

21 Donald F. Kettl, *Managing Risk, Improving Results: Lessons for Improving Government Management from GAO's High-Risk List,* IBM Center for The Business of Government, 2016.

22 Hardy, *Enterprise Risk Management,* 42.

23 Ibid, 44.

24 Robert Greer and Justin Bullock, *Risk Management and Reducing Improper Payments: A Case Study of the U.S. Department of Labor,* IBM Center for The Business of Government, 2017.

25 *Improper Payments Elimination and Recovery Act of 2010,* Public Law 111-204 (July 22, 2010).

26 Stanton and Webster, *Managing Risk and Performance,* 116.

27 Webster and Stanton, *Improving Government Decision Making,* 12-13.

28 Ibid, 16.

29 Association for Federal Enterprise Risk Managers, *Enterprise Risk Management in the Public Sector: 2015 Survey Results.* 2015, 3.

30 Ibid, 14.

31 Hardy, *Managing Risk in Government*, 33.

32 Stanton and Webster, *Managing Risk and Performance,* 140.

33 Hardy, *Managing Risk in Government,* 35.

34 Ibid.

35 Stanton and Webster, *Managing Risk and Performanc*e, 143.

36 Alan Thompson, *Managing a Responsive Supply Chain in Support of U.S. Military Operations: Interview with VADM Alan Thompson, Director, U.S. Defense Logistics Agency,* interview by Michael J. Keegan, The Business of Government Hour, *Federal News Radio*, April 2009.

37 Stanton and Webster, *Managing Risk and Performance,* 182.

38 Sara Moore, *Risk and Reward, Loglines,* Defense Logistics Agency, March-April 2010, 4.

39 Ibid, 3.

40 "Enterprise Risk Management—Integrated Framework," Committee of Sponsoring Organizations of the Treadway Commission, accessed June 6, 2018, https://www.coso.org/Pages/erm-integratedframework.aspx and International Standards Organization: ISO 3100:2009 Risk Management – Guidelines," 2009, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en.

41 U.S. Department of Commerce, *Guide for Applying the Risk Management Framework to Federal Information Systems,* 2010.

42 Rajni Goel, James Haddow, and Anupam Kumar, *A Framework for Managing Cybersecurity Risk,* The IBM Center for The Business of Government, 2018.

43 Transportation Security Administration, *Enterprise Risk Management: ERM Policy Manual,* August 2014, 9.

44 Stanton and Webster, *Managing Risk and Performance,* 164.

45 Office of Management and Budget. *Circular A-11, Preparation, Submission and Execution of the Budget Part 6,* Section 270, 2014.

46 Karen Hardy, *Interview with Karen Hardy, Deputy Chief Risk Management Officer, U.S. Department of Commerce,* interview by Michael J. Keegan, The Business of Government Hour, *Federal News Radio*, August 22, 2016.

47 Karen Hardy, *Enterprise Risk Management* 2015, 5.

48 Jason Miller, "OMB to Require Agencies to Measure Risk at the Enterprise Level"*, Federal News Radio*, October 17, 2014.

49 These challenges are gleaned from two IBM Center for The Business of Government reports, *Managing Risk in Government: An Introduction to Enterprise Risk Management,* 2010, and *Improving Government Decision Making through Enterprise Risk Management*, 2015.

50 Office of Management and Budget, *Circular No. A-11: Preparation, Submission, and Execution of the Budget,* August 1, 2017.

51 Charles Clark, "OMB Prepares to Ratchet Up Enterprise Risk Management," *Government Executive*, February 29, 2016.

52 Office of Management and Budget, *Circular No. A-123: Management's Responsibility for Enterprise Risk Management and Internal Control,* July 15, 2016, 7.

53 Office of Management and Budget, *Circular No. A-123,* Section 2, 9.

54 U.S. Chief Financial Officers Council. *Playbook: Enterprise Risk Management for the U.S. Federal Government*, 2016. p.6 and U.S. Government Accountability Office. *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk,* GAO-17-63, Dec. 1, 2016.

55 U.S. Chief Financial Officers Council. *Playbook: Enterprise Risk Management for the U.S. Federal Government,* 2016. p.6.

56 U.S. Government Accountability Office. *Enterprise Risk Management: Selected Agencies'Experiences Illustrate Good Practices in Managing Risk,* GAO-17-63, Dec. 1, 2016.

57 Office of Management and Budget, M-18-15: 2018 *Strategic Review Guidance,* April 24, 2018.

58 These lessons are derived from the following IBM Center for The Business of Government reports: *Managing Risk in Government: An Introduction to Enterprise Risk Management,* 2010, *Improving Government Decision Making through Enterprise Risk Management,* 2015, and *Risk Management for Grants Administration: A Case Study of the Department of Education,* 2015.

59 Claire MacRae and John Houston, *Setting the Risk Agenda: Exploring the Future of the Risk Management Profession,* Institute of Risk Management, 2016, 5.