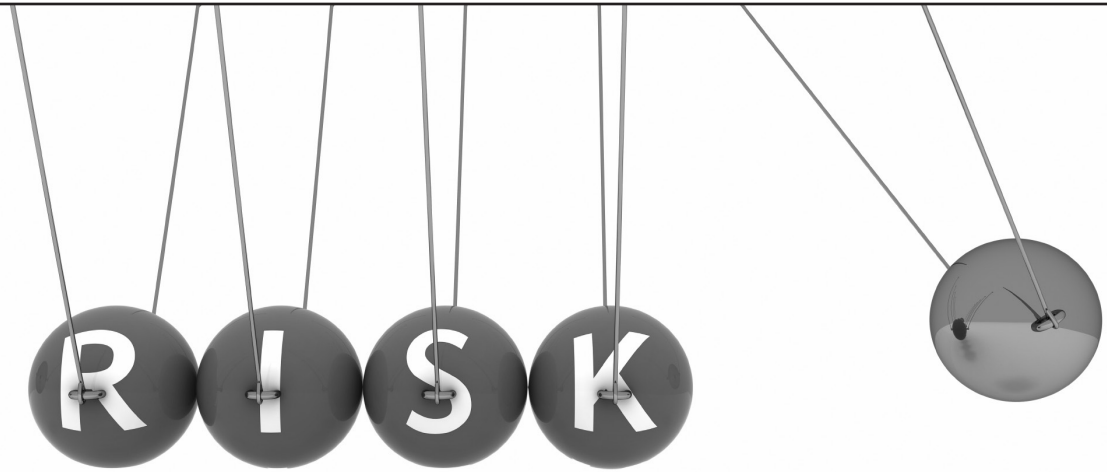


Financial Management Series

# Managing Risk in Government: An Introduction to Enterprise Risk Management



Dr. Karen Hardy



IBM Center for  
The Business of Government

2010  
Second  
Edition

FINANCIAL MANAGEMENT SERIES

# **Managing Risk in Government: An Introduction to Enterprise Risk Management**

**Dr. Karen Hardy**



# TABLE OF CONTENTS

<b>Foreword</b> .....	5
<b>Executive Summary</b> .....	7
<b>Introduction</b> .....	10
Risk Management: What It Is and Why It Matters .....	10
Evolution of Risk Management .....	11
<b>Why Enterprise Risk Management in the Federal Government?</b> .....	13
Limitations to ERM .....	14
ERM Frameworks .....	15
Building a Risk Culture: ERM Behaviors, Skills, and Competencies.....	17
<b>Risk Management in Federal Agencies</b> .....	19
U.S. Federal Government Policy on Risk Management.....	19
Examples of Risk Management in the Federal Government.....	21
<b>Applying Risk Management in Government: Centers for Disease Control and Prevention</b> .....	29
CDC Approach to ERM.....	29
Key Drivers of ERM at CDC.....	32
ERM Governance Structure at CDC.....	32
<b>Applying Risk Management in Government: Department of Education</b> .....	33
Federal Student Aid .....	33
The ERM Governance Structure.....	36
Insights from the FSA Experience.....	38
<b>Findings and Recommendations</b> .....	39
Findings.....	39
Recommendations.....	41
<b>Appendix: Survey of Risk Management Skills</b> .....	43
<b>Endnotes</b> .....	45
<b>References</b> .....	46
<b>Acknowledgements</b> .....	48
<b>About the Author</b> .....	49
<b>Key Contact Information</b> .....	50



## F O R E W O R D

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, “Managing Risk in Government: An Introduction to Enterprise Risk Management,” by Karen Hardy. The report is especially timely because of the Obama administration’s focus on accountability and transparency which has prompted a renewed focus on risk and controls. In addition, recent high-profile financial failures have also focused increased attention on risk and controls.

In recent years, the federal government has been on the receiving end of new legislation and regulations that require it to better manage risk and improve controls in discrete areas. Generally, to comply with the requirements of each of these new mandates, agencies have put into place stovepiped compliance programs. This stovepiped approach to compliance is costly and does not optimize value. This report explores how federal chief financial officers (CFOs) and financial managers can help guide their agencies to take a more holistic approach to risk management by implementing an Enterprise Risk Management (ERM) system. This approach helps reduce the total cost of compliance, while helping agencies achieve greater value from their risk management activities.

Although the current focus on risk management for most federal CFOs and financial managers stems from the American Recovery and Reinvestment Act (ARRA) of 2009 and the revised OMB Circular A-123, these are only two requirements of many that federal agencies must address. Agencies are also required to report their results in implementing Federal Managers’ Financial Integrity Act (FMFIA) of 1982, Improper Payments Information Act (IPIA) of 2002, and the Federal Information Security Management Act (FISMA) of 2002, among others. Virtually all of these requirements are ultimately geared toward one objective—improved risk management—so an agency’s response to risk provides reasonable assurance that the organization will achieve its strategic objectives.

This dramatic increase in compliance requirements, coupled with the realization that compliance cannot be effectively achieved by just having discrete compliance programs in various business units, makes it now critical for organizations to move toward an enterprise-wide risk management approach. Holistic ERM starts with a focus on the possible events that could potentially happen and their classification into opportunities and risks.



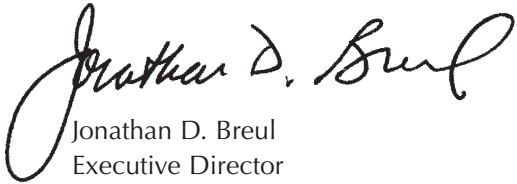
Jonathan D. Breul



Denise Rabun

Keeping track of these possible events requires good data and data governance managed at the enterprise level. It also requires a taxonomy or classification scheme of the most important risks to the entity and a common language for understanding those risks. Improved data management allows the enterprise to take advantage of modern analytical methods in order to quantify the impact of risk. Data analysis also enables the enterprise to gain an overall view of current risk, as well as trends and potential future risks.

It's clear that implementing an ERM approach makes sense and yields benefits to an organization. It is our hope that federal executives will find this report useful to them as an introduction and guide to Enterprise Risk Management.



Jonathan D. Breul  
Executive Director  
IBM Center for The Business of Government  
jonathan.d.breul@us.ibm.com



Denise Rabun  
Public Sector Financial Management  
Partner, IBM Global Business Services  
denise.rabun@us.ibm.com

## EXECUTIVE SUMMARY

Risk management is not a new concept within the federal sector. What is new is the need to integrate risk management into the strategic and decision-making processes that cut across the organization, and abandon the outdated practice of managing risks within functional silos and stovepipes. The purpose of this paper is to provide federal managers with an overview of ERM and what should be considered when implementing ERM.

Enterprise Risk Management (ERM) has been recognized as the process for making this integration work. ERM is defined as

*“a process, effected by an entity’s ... management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives” (COSO, 2004).*

While there is great expectation and hope for this management practice, there are very few success stories and best practices available in the federal sector to benchmark. This is due in part to the multiplicity of missions and objectives of government agencies, which makes it difficult to achieve a uniformed approach to ERM. However, this is not a problem unique to the federal arena. In a recent Enterprise Risk Oversight Survey conducted by the ERM Initiative at North Carolina State University, of 700 entities surveyed across a broad range of industries, 44 percent of respondents said that they had no enterprise-wide risk management process in place and have no plans to implement one (Beasley, Branson, Hancock, 2009).

The lack of a standard methodology across the federal sector need not discourage agencies from implementing ERM, as variations in ERM are expected. This is evidenced in the approaches of the agencies featured as case studies in this report: the Centers for Disease Control and Prevention and the Department of Education’s Federal Student Aid. Each agency brings a unique perspective to ERM, driven by different goals and objectives. Yet, despite these differences, each agency’s approach uses the general concepts and context of ERM, whether using specific frameworks, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Integrated Framework or the Canadian Integrated Risk Management Framework, as working models.

Benefits of ERM include:

- Gaining a cultural understanding of the importance of sustaining high credibility as an agency
- Affording the opportunity for agencies to make more educated decisions
- Increasing knowledge and understanding of risk across the organization
- Improving risk culture
- Aligning risks with agency/program goals and objectives
- Providing for a more efficient and effective means of managing risk
- Agreeing on core values and on the necessity for a broadly integrated risk management approach

Challenges of ERM include:

- Providing the appropriate foundation, assessment, and management platform



- Insufficient sponsorship of ERM at the executive level
- Positioning ERM as a strategic management practice and not as an additional task
- 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
- Federal government regulations and requirements
- Lack of understanding about risk management
- Lack of qualified risk management professionals and expertise
- An internal competitive culture prone to stovepiping
- Aligning risk reward and incentive programs with strategic objectives

## Best Practices of Federal Agencies

When implementing ERM, government leaders should keep in mind the following hands-on best practices identified by the agencies featured in this report:

### Getting Started

- Develop a risk management lexicon to ensure consistency of terminology across the organization
- Establish a communications plan and stick with it
- Don't underestimate the level of effort or short-change the planning process
- Customize ERM strategy, approach, and methodology based on the specific requirements of your organization
- Ensure support from senior leadership which is critical to effectively identifying and addressing risks and opportunities
- Train your employees

### Organizing for ERM

- Establish a Risk Office or ERM organization
- Have a dedicated "risk champion" with good communication skills
- Ensure that the head of the risk organization/ "risk champion" is a member of executive management

- Establish and maintain executive level support, ideally from the highest levels in the organization

### Operating an ERM Program

- Develop a policy that outlines the organization's expectations regarding the management of risks
- Document the process and analysis so that it can be replicated
- Provide specific examples of risks tailored to the organization to help the learning process
- Reward risk identification, don't penalize it; and this is critical to changing the culture and effectively establish an agency-wide ERM process
- Engage those who manage risks, as well as areas with inherent risks, to develop analytical tools and recommendations. These stakeholders often know the consequences of effective and ineffective risk management, and have the rigor in thinking and planning to address risks
- Link risk training to business results, where possible
- Seek diverse perspectives on issues, as they are critical to risk and opportunity management

Despite the important benefits that ERM provides, limitations do exist. As noted by COSO, "limitations result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures, controls can be circumvented.... And management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives" (COSO 2004).

## Recommendations

Based on the findings in this study, the following recommendations are offered:

1. **Establish short- and long-term strategic plans for ERM.** ERM effectiveness is a matter of maturity. It takes time. Make sure stakeholders understand that ERM is a process that is strengthened over time.
2. **When considering ERM, agencies must establish a tone at the top within the organization.**

Without senior leadership support, it will be difficult to get buy-in throughout the organization. Thus, ERM will be seen as yet another task and paper exercise rather than as a strategic management process.

3. **When adopting ERM, make sure the benefits are communicated to stakeholders.** Besides the need for compliance, demonstrate how ERM can enhance organizational performance, heighten awareness about risk management, improve workforce skill sets, and create a “safe place” for managers to discuss risk management outside of their comfort zones.
4. **Collaborate within and across other agencies.** Don’t work in a vacuum. Find agencies with similar operational functions or missions and benchmark risk management practices. Join organizations that advocate ERM and provide resources for continuous learning in this subject matter (e.g., [FederalERM.com](http://FederalERM.com)).
5. **Don’t reinvent the wheel.** Use what you have. If there is an existing internal control framework in place, build upon that. Strategize about how ERM can enhance or strengthen your existing internal control environment.
6. **Have experienced staff available to champion and carry out the vision of the ERM process.** A knowledgeable workforce is the key to successful ERM implementation. If you cannot hire new staff, retrain the staff that you have.
7. **Communicate short wins immediately.** Nothing reinforces success like results. Show stakeholders how ERM has led to successful identification and mitigation of risks, business opportunities or cost savings.

# Introduction

*“Understanding and managing risk is essential for any organization, public or private. In the private sector, risk management is a widely accepted practice designed to control risks that could lead to a business failure if not properly managed. Therefore, profit maximization is the end result. However, the application of risk management is not as straightforward in the public sector. Government managers must manage risk within a complex environment taking into consideration the diverse missions and multiple objectives of public agencies. Rather than seeking to realize the greatest profit, government leaders must strive to manage risk that increases the likelihood of an agency achieving its primary mission and strategic objectives.”*

Treasury Board of Canada Secretariat, 2001

## Risk Management: What It Is and Why It Matters

Risk is unavoidable. It transcends virtually every human situation and is present in our daily lives and within public and private sector organizations. While there are many acceptable definitions of risk in use across various industries and organizations, the most common concept in all definitions is the uncertainty of outcomes (Treasury Board of Canada Secretariat, 2001).

The various definitions of risk also depend on how outcomes are characterized. For some organizations, risk has been affiliated only with adverse consequences without taking into consideration the upside (or opportunities) to risk. Yet, there continues to be a debate and discussion on what would be an acceptable generic definition of risk that captures both the associated consequences and opportunities. In addition to consequences, one school of thought asserts that, when assessed and managed properly, risk can lead to innovation as well. A perspective that supports this notion is the significant role the federal government’s new chief performance officer (CPO) can play in managing risk opportunity.

As a key executive, the new CPO will be responsible for streamlining government processes, cutting program costs, and finding best practices that can lead to more effective management of resources. A stated goal of the Obama administration is to eliminate dozens of government programs shown to be wasteful or ineffective. Some experts note that, if approached appropriately, the CPO can capitalize on risk opportunities by identifying those programs that “manage people’s risks the best,” saving taxpayers millions of dollars.

A “success indicator for government programs could be how well they spread, shift and or reduce public risk as defined by the agency’s mission statement. Another measure could include whether the benefits of mitigating the risk outweigh the program’s cost,” wrote Robert Charette, a risk management expert and founder of the ITABHI Corporation, which specializes in organizational risk management issues. “In addition, if a program is to be closed down because it doesn’t work, the CPO could reason that the government was mismanaging the public’s risk or that the agency wasn’t equipped to oversee the risk in the first place,” wrote Charette.

Whether adverse or opportunistic, the bottom line is that there is currently no standard definition of risk established within the U.S. federal government. Some experts argue that leading risk management begins with establishing a common definition of key risk concepts so that risk management approaches are implemented consistently across an enterprise. According to Mark Beasley, Deloitte Chair and director of North Carolina State University's Center for Enterprise Risk Management, "Providing clear definitions of risk terms (including discussion of whether 'risk' represents both risk opportunities and risk threats) is often the required first step in establishing an enterprise risk management (ERM) process." (Beasley, Branson and Hancock 2008). For the time being, a refined definition is a continuously evolving process within the U.S. federal sector.

In contrast, the Public Service in Canada has gained consensus on a definition of risk as a part of its Integrated Risk Management Framework. Issued in 2001, the framework is a practical guide to assist Canadian public service employees in their decision-making processes. At the organizational level, it helps departments and agencies to think more strategically and improve their ability to set common priorities. At the individual level, it helps all employees to develop new skills and strengthens their ability to anticipate, assess, and manage risk.

## Evolution of Risk Management

Effective risk management cannot be practiced in isolation, but needs to be built into existing decision-making structures and processes (Peter, Gjerdrum & Peeling, 2009). In the past, risk management was seen as relating mainly to matters of safety and insurance. Over time, this systematic approach has evolved from a transactional functional to that of a strategic nature (Peter, et al.).

Previous practices viewed risks as threats and focused on avoidance of negative events, treated risk as a separate function, and continuously managed risk independently within silos. Gradually, organizations began to integrate risk by accepting risk as an expense, shifting their focus to managing risk, and recognizing risk managers as risk owners. Strategically, companies are now working towards a broader view of risk, understanding that risk is an

## Definition of Risk

### Public Service of Canada

**Risk:** "Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives."

**Risk Management:** "... a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues."

**Source:** Integrated Risk Management Framework, *Treasury Board of Canada Secretariat, April 2001*

### U.S. Government Accountability Office (GAO)

**Risk:** "An event that has a potentially negative impact and the possibility that such an event will occur and adversely affect an entity's assets, activities, and operations."

**Risk Management:** "The 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. 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. Risk management addresses risk before mitigating an action, as well as the risk that remains after countermeasures have been taken."

**Source:** *Government Accountability Office, Report # GAO-06-91, December 2005*

uncertainty, shifting the focus to optimizing risk and advocating risk managers as risk facilitators and leaders.

Building on the evolution of risk management, ERM recognizes that risks can be threats and opportunities, and are a corporate-wide daily concern that is embedded in the operations. ERM transforms risk management from a silo approach to a holistic approach that is coordinated at the highest level within the organization and that recognizes the value of tangible and intangible assets. Historically, organizations focused on hazard risk management and insurable financial risks. Today, the practice is much more encompassing, covering operational, strategic, financial, and reputation risks.

## Glossary of Risk Management Terms

**Source:** GAO Risk Management Framework (GAO, 2005) and ISO/FDIS 31000 International Standard Final Draft (July 25, 2009).

**Consequence:** The expected worse case or reasonable worse case impact. This loss or damage may be long or short term in nature.

**Monitoring and evaluation:** A continuous repetitive assessment process to keep a risk management process current and relevant. It includes, among other activities, external peer review, testing, and validation.

**Opportunity cost:** The value of opportunities forgone.

**Risk:** An event that has a potentially negative impact and the possibility that such an event will occur and adversely affect an entity's assets, activities, and operations.

**Risk appetite\*:** Amount and type of risk that an organization is prepared to pursue, retain or take.

**Risk assessment:** The process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact.

**Risk identification\*:** The process of finding, recognizing and describing risks. Risk management: 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. Risk management addresses risk before mitigating action, as well as the risk that remains after countermeasures have been taken.

**Risk management:** 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. Risk management addresses risk before mitigating action, as well as the risk that remains after countermeasures have been taken.

**Risk management framework\*:** A set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, review and continually improving risk management throughout the organization.

**Risk owner\*:** A person or entity with the accountability and authority to manage the risk.

**Risk profile\*:** A description of any set of risks. (The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined).

**Residual risk\*:** The risk remaining after risk treatment. Residual risk can contain unidentified risks and can also be known as "retained risk".

**Risk treatment\*:** Process to modify risk. Risk treatment can involve: (1) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk (2) taking or increasing risk in order to pursue an opportunity (3) removing the risk source (4) changing the likelihood (5) changing the consequences (6) sharing the risk (7) retaining the risk.

**Stakeholder\*:** A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

\* © ISO. This material is reproduced from ISO DIS 31000 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). ISO DIS 31000 is not an approved ISO standard and it cannot be referred to as such. This material is subject to change without notice. No part of this material may be copied or reproduced in any form, electronic retrieval system or otherwise or made available on the Internet, a public network, by satellite or otherwise without the prior written consent of the ANSI. Copies of all ISO standards may be purchased from the ANSI, 25 West 43rd Street, New York, NY 10036, (212) 642-4900, <http://webstore.ansi.org>.

# Why Enterprise Risk Management in the Federal Government?

The U.S. government has a long history of adapting and adopting successful and prudent business practices from the private sector. In the arena of financial management, this is perhaps best illustrated by the adoption of the Chief Financial Officers Act of 1990, with its requirement that federal agencies pass financial audits (Beasley, Branson & Hancock, 2008). The adoption of Enterprise Risk Management (ERM) is no exception. While risk management has long been a priority for many organizations, the recent private sector financial collapse has put a spotlight on enterprise risk management as a critical component of an organization's overall health and long-term sustainability (Fox, 2009). ERM is defined as

*“a process, effected by an entity's ... management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives” (COSO, 2004).*

Embedded in this definition are seven fundamental concepts which assert that ERM is (COSO, 2004):

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in a strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity, and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

When put into context, the general idea is that “ERM is a process that works well at all levels in an organization and brings together the business, back office, and top strategic layers in an integrated manner. By definition, a process is immersed in the business and does not sit outside of the real work. ERM is not about setting up a new team to do ERM. It is about getting a process that feeds into the main business lines to add value and make a meaningful contribution to the bottom line” (Pickett, 2006).

Furthermore, ERM is an initiative that is championed by the highest level of management, driven down into the organization. ERM promulgates that “if risk is built into the equation when setting strategy for the entire business, then risk management can become a holistic process that starts at the top and filters its way down through the enterprise” (Pickett, 2006).

In response to the public's demand for change, government managers as well as those within the private sector are looking for ways to weave risk management strategies and tactics into their everyday operations and strategic decisions at the highest level. Federal agencies are now beginning to recognize the need to weigh the probabilities of what could go wrong before it happens, the upside of doing a cost-benefit analysis for mitigating or accepting a risk, and the advantages of discussing, evaluating, and feeding risk into an agency's strategic plan and budget regardless of the mission. ERM is fast becoming an important activity for many

agencies to undertake as a solution for bringing various agency risk activities all together.

While traditional risk management has its merits, it is often still carried out in silos and stovepipes within organizations, leaving the “white spaces” between organizational functions “open to interpretation.” ERM challenges the status quo and requires managers and leaders to step out of their organizational comfort zones and into a collaborative environment to discuss not only common risks, but uncover latent risks as well. As part of ERM, the white spaces also indicate that there is room to discuss risks that do not necessarily fit into one particular functional area, but requires perspective from every function in order to properly address an enterprise-wide issue that could impact the organization’s mission and strategic objectives.

## Limitations to ERM

ERM, if done effectively, has the potential to bring the white spaces and current risk activities being undertaken within each silo together in a process that will benefit the organization as a whole and raise the discipline to a more strategic level within the organization. However, limitations do exist. “Limitations result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures, controls can be circumvented.... And management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance as to achievement of the entity’s objectives” (COSO, 2004).

Freddie Mac is an example of how the benefits of ERM can be overcome by organizational breakdowns and disconnects. Armed with a well-trained workforce, Freddie Mac touted its approach to ERM. Yet, despite having the right people and skills in place, it failed to manage the highest risks to its mission, goals, and strategic objectives.

Prior to the meltdown, Freddie Mac was a “model dependent” business, in that a separate organization was established to focus on its key risk areas. As part of its model, there was an organization that focused on credit risk, market risk, operational risk, and mod-

## The Committee of Sponsoring Organizations (COSO)

The Committee of Sponsoring Organizations (COSO) is a voluntary private sector organization comprised of the following professional associations: American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Management Accountants (IMA), and the Institute of Internal Auditors (IIA). COSO is known worldwide for providing guidance on critical aspects of organizational governance, business ethics, internal control, ERM, fraud, and financial reporting.

COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

COSO is dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices.

**Source:** *COSO.org*

els risk. Freddie Mac’s operational risk central function sat in the ERM Oversight Division. Within the function, there were about 20 employees who reported to the chief enterprise risk officer, who in turn reported to the CEO. Operational risk managers were also embedded in the business line functions of the organization as well. In all, 40 employees were exclusively assigned to the operational risk function within the organization.

However, there are instances where ERM can and does help companies perform better. In a recent ERM study, it was found that organizations that have embraced ERM have realized a concrete advantage in their risk management competency. The study also found that 93 percent of organizations with formalized ERM programs in place make better risk-informed decisions—a recognized competitive advantage over those that do not have an ERM program (RIMS, 2009).

Goldman Sachs is one company that portrayed that competitive advantage. Prior to 2008, while many financial companies were taking uncalculated risks, Goldman Sachs adjusted its positions in mortgage-backed securities, differentiating itself from the rest of the market at a time when some might have criticized the move as excessively cautious. Described as the “perfect storm” in the financial sector, David Solomon, Partner and Member of Goldman Sachs’ Management Committee, attributed the company’s resilience to their risk management competencies – that is, a strong governance oversight, reporting process, communications, and culture (Solomon, 2008).

### ERM Frameworks

As federal managers move toward strengthening risk management processes within their agencies, more frameworks will be needed to help navigate the complexities of a risk system. Here are a few to consider:

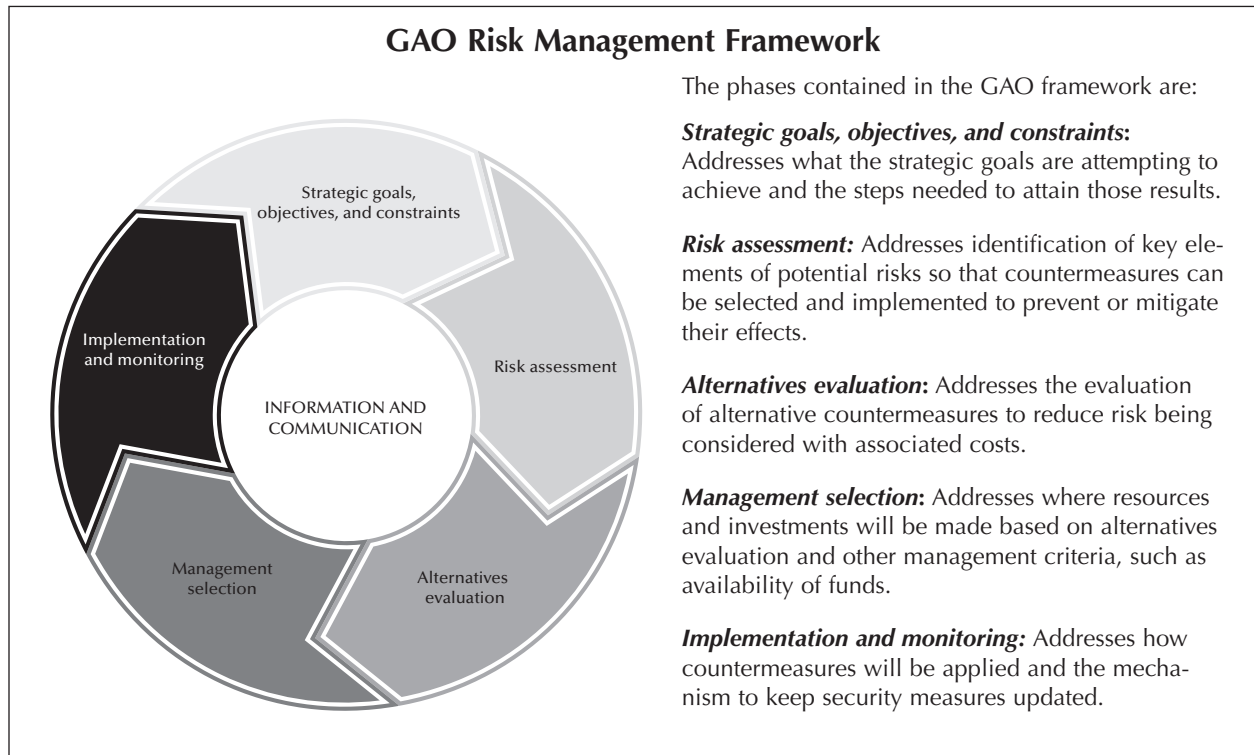
#### GAO Risk Management Framework<sup>1</sup>

The GAO Risk Management Framework (GAO, 2005) was developed using several resources, including the Government Performance and Results Act (GPRA) of 1993, the Government Auditing Standards, 2003 Revision, GAO’s Standards for Internal Control in the

Federal Government (November 1999); guidance from the Office of Management and Budget (OMB); the work of the President’s Commission on Risk Management; white papers; and the ERM approach of the COSO. The framework was field-tested on several GAO reviews and is considered a starting point in a field that is evolving; the entire cycle of risk management activities should be viewed as a goal.

The framework has been developed so that individual phases of the approach, such as risk assessment, do not become ends in themselves, but provide a full cycle of related activities; from strategic planning through implementation and monitoring. The process is dynamic, and although the various phases appear linear, new information can be entered at any phase.

The GAO framework can be used to inform agency officials and decision makers of the basic components of a risk management system or can be used as a stand-alone guide. It is designed to be flexible, in that the approach may be applied at various organizational levels ranging from that of a department of a multiagency organization down to that of a specific project or program. Because there is no one uniformly accepted approach to risk management,



Source: Government Accountability Office, Report # GAO-09-687



terms and activities may differ across organizations (GAO, 2005).

### **International Standard 31000 (ISO 31000)<sup>2</sup>**

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies. A new standard issued by this organization, ISO 31000, provides a standard risk management framework for use across various entities, sectors and organizations. While all organizations manage risk to some degree, ISO 31000 establishes a number of principles considered essential to make risk management effective. Published in November of 2009, ISO 31000 is the first international standard on the practice of risk management. The standard applies to any type or size organization in any country (Gjerdrum, 2009).

It is expected that this standard will be widely adopted as the norm for risk management practices, though it is not intended to be a compliance standard. Implementation is strictly voluntary. However, the US Technical Advisory Group (US TAG), which reviewed and commented on the standard before its final publication, has approved ISO 31000:2009 as the standard for the practice of risk management in the United States.

ISO 31000 recommends that organizations develop, implement, and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values, and culture.

"For traditional risk managers in the U.S., it is important to remember that this new standard is intended to build upon what you already do well and expand your view about risk," says Dorothy Gjerdrum, Chair of the U.S. Technical Advisory Group.

According to Gjerdrum, the U.S., up to this point, has been creative and forward-thinking about risk finance and risk transfer techniques, but not as forward-thinking about identifying a broad range of risks (beyond insurable risk, beyond hazard identification, beyond emergency planning or disaster preparedness) or addressing cumulative or crossover risks (such as IT or pandemic planning).

"A real strength of this new approach is the identification of risk owners and the necessary widespread education about risk — both inside and outside your organization. It increases accountability and strengthens communication," says Gjerdrum. "The link to business objectives (at all levels) strengthens both the relevance and the importance of risk management. Ultimately, it will make risk management central to the success of an organization, and an intimate part of key processes such as planning, management and governance," says Gjerdrum.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently, and coherently across an organization. The generic risk management approach described in ISO 31000 provides principles and guidelines for managing any form of risk in a systematic, transparent, and credible manner and within any scope and context. This international standard has the potential to meet the needs of a wide range of stakeholders, including:

- Those responsible for developing risk management policy within their organization
- Those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project, or activity
- Those who need to evaluate an organization's effectiveness in managing risks
- Developers of standards, guides, procedures, and codes of practice that—in whole or in part—set out how risk is to be managed within the specific context of the documents

Similar to the COSO and GAO frameworks, the ISO 31000 standard provides a holistic view of risk management with familiar terms and processes. However, as a generic standard, it will have a much broader appeal and application across multiple industries, including the government.

### **COSO ERM-Integrated Framework**

The COSO ERM is a landmark document issued in September 2004, and provides a set of standards that elevated risk management to a higher level in the

### Three Dimensions of COSO ERM

#### Organizational Objectives

- Strategic
- Operations
- Reporting
- Compliance

#### Management Operations

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information
- Communication
- Monitoring

#### Entity Units

- Subsidiary
- Business unit
- Division
- Entity-level

business arena. COSO provides a three-dimensional model that ERM encompasses.<sup>3</sup>

The three dimensions can be categorized as Organizational Objectives, Management Operations and an Entity's Units. Organizational Objectives are important because "risk is only present where it impacts an organization's objectives." This dimension says that "ERM is about four main considerations that mean an enterprise views risk at a strategic level, within operations, with full consideration of corporate reporting and obligations and also the field of compliance with laws, regulations, and procedures" (Pickett, 2006).

Management Operations provides a risk cycle for starting the process. It is comprised of eight interrelated components derived from the way management runs an enterprise and is integrated with the management process (COSO, 2004, p. 3). ERM is not a serial process, where one component only affects the next. Rather, "it is a multidirectional, iterative process in which almost any component can and does influence another" (COSO, 2004).

In the past, the COSO ERM framework has been the primary source for federal managers seeking to understand the key components of a risk management system. However, many public sector managers found the framework difficult to implement because it didn't speak to the language of government, such as "providing effective programs and services" rather than "improving profit margins," the focus of the private sector companies. In the last few years, additional frameworks and standards have emerged that closely relate to the business operations of public sector organizations. The GAO Risk Management Framework and the draft ISO 31000 are two resources that could be helpful models for advancing risk management within the public sector.

### Building a Risk Culture: ERM Behaviors, Skills, and Competencies

*"The test in the real world is how competent the organization's risk management practices are, and the degree to which [organizations are] instilling risk management behaviors into its culture and management's decision-making [process]. In short, how mature is the company's enterprise risk management program and how thorough are its' practices at all levels of the organization?"*

—RIMS, 2009

The Freddie Mac crisis is a subtle reminder that the mere implementation of enterprise risk management activities is not enough to protect an organization from system-wide failures. Rather, it is imperative that organizations develop a culture of risk management where a positive orientation towards the business discipline is embedded into the day-to-day operations of the organization. Essentially, "the key to successful enterprise risk management practices depends on the behavioral attributes of the organization at all levels." (RIMS, 2009).

Citing the financial crisis at Citigroup, AIG, Freddie Mac and Fannie Mae, the Risk and Insurance Management Society (RIMS) contends that of three possibilities "the financial crisis resulted from a ... failure to embrace appropriate enterprise risk management behaviors—or attributes—within these distressed organizations" and not so much "from a failure of risk management as a business discipline" (RIMS, 2009).

### Risk and Insurance Management Society (RIMS)

RIMS is a not-for-profit organization dedicated to advancing the practice of risk management. Founded in 1950, RIMS represents more than 3,500 industrial, service, nonprofit, charitable, and governmental entities. The Society serves more than 10,000 risk management professionals around the world.

*Source: RIMS.org*

Several frameworks and standards have been designed to help organizations institutionalize risk management as a business discipline. RIMS does not advocate a particular ERM framework and suggests that any one can work effectively. However, it does preclude that, despite the standard, guideline or framework used, “the key to successful ERM practice depends on the level of maturity the organization demonstrates in seven behavioral attributes” (RIMS, 2009):

1. Adoption of an ERM-based approach
2. ERM process management
3. Risk appetite management
4. Root cause discipline
5. Uncovering risks
6. Performance management
7. Business resiliency and sustainability

The seven attributes are a part of the RIMS Risk Maturity Model (RMM) for ERM assessment. The RMM is a foundational tool used by executives and others “charged with risk management responsibilities to design sustainable ERM programs” reflective of their organizations’ strategy and short and long-term business objectives (RIMS, 2008b). The model consists of 68 key readiness indicators that describe 25 competency drivers for the 7 attributes that create ERM’s value and utility in an organization. The RMM also allows companies to “assess their current practices against these validated risk competencies and create a roadmap to achieve whatever level they desire.”

According to the RIMS State of ERM Report 2008, based on responses from 564 companies globally,

the least mature attributes within organizations include risk appetite and risk tolerance, root cause discipline, and performance management. As noted by RIMS, if several of the key enterprise risk management behavioral attributes were designed and implemented comprehensively and systematically, many of the losses suffered by these organizations “could have been identified and mitigated, if not prevented.”

Within a risk culture, behavioral attributes are also key and applicable at the individual level as well. RIMS emphasizes that in order to drive and sustain a risk program and practice sound risk management, those responsible for leading risk activities within an organization need to develop a specific set of competencies and skills.

The RIMS Core Competency Model (RIMS, 2007) illustrates the broad suite of skills needed. For the purposes of this study, a Federal Risk Management Core Competency Survey was designed and distributed to agency leaders engaged in the preliminary stages of ERM. The purpose of the survey was to determine what knowledge, skills, and resources are needed to successfully implement and sustain ERM within a government agency. The findings of this survey are discussed in the Appendix.

# Risk Management in Federal Agencies

## U.S. Federal Government Policy on Risk Management

ERM is in its infancy within the United States government. Other governments, such as that of Canada, established a national policy surrounding ERM nearly a decade ago. Canada's Integrated Risk Management Framework aims to protect the public interest and maintain public trust. The Canadian framework is part of its larger objective to modernize management practices in order to make the government more citizen-focused and able to meet the changing needs and priorities of its community (Treasury Board of Canada Secretariat, 2001). Canada provides a model for managing and integrating risk management into existing decision-making structures and processes.

Even though the U.S. does not have a national risk management policy, agencies must comply with the Federal Manager's Financial Integrity Act (FMFIA) of 1982 and OMB Circular A-123, "Management's Responsibility for Internal Controls". Both directives require agencies to maintain robust internal control structures that ensure:

- Effective and efficient operations
- Compliance with applicable laws and regulations
- Reliable financial reporting

Most Chief Financial Officers (CFO) focus on A-123's Appendix A, that pertains to internal control over financial reporting. However, financial reporting is only one of three control objectives under Section 2 of the FMFIA. The other two are effectiveness and efficiency of operations and compliance with applicable laws and regulations (Association of Government Accountants [AGA], 2008).

## Other International Standards and Risk Policies

**Canadian Risk Management Policy.** Issued in 1994, the objective of this policy is to safeguard the government's property, interests, and certain interests of employees during the conduct of government operations. Departments within the Public Service of Canada are required to identify, minimize, and contain risks and to compensate for, restore and recover from risk events. The Canadian risk management process includes the following phases:

- Identifying Issues, Setting Context
- Assessing Key Risk Areas
- Measuring Likelihood and Impact
- Ranking Risks
- Setting Desired Results
- Developing Options
- Selecting a Strategy
- Implementing the Strategy
- Monitoring, Evaluating and Adjusting

**Australian/New Zealand Risk Management Standard (Source: RM Guidelines AS/NZS 4360: 2004).**

This framework first emerged in 1999 and was re-released in 2004. It is likely to be replaced by ISO 31000. The AS/NZ RM Standard is simplified, has a linear diagram, and consists of clear language. The Standard emphasizes communication and monitoring throughout the Risk Management process and specifically addressed analysis of opportunities.

**British Risk Management Code of Practice (Source: BSI British Standards-BS 31100: 2008).** The British RM Code perspective emphasizes the future direction of the business; turning strategy into action including program, project and change management, and the day-to-day operations including people, processes, and information security.

*Source: Peter. et. al*

The policy requirements and processes are very prescriptive for conducting risk assessments pertaining to internal controls over financial reporting but falls short in (1) outlining specific steps for evaluating, testing, and assessing risks associated with administrative and federal program operations, and (2) demonstrating how risk assessment ties into the overall process for managing risk at an enterprise level. The shortcomings have left many agencies grappling with approaches to incorporate these administrative and programmatic requirements, but not without hope.

According to an annual CFO Survey, some executives want to see Appendix A requirements reduced or unchanged, sensing that a better return on investment would be the re-channeling of resources to control over program and entity performance and related reporting (AGA, 2008). “Complying with FMFIA aside, sound controls on operations reduce the risk of poor performance of an entity’s mission. That is more important than getting the financial numbers right, and should receive as much or more attention as controls over financial reporting. It is also where CFOs can broaden their roles and increase the value they add to an entity” (AGA, 2008).

However, not all financial executives are enthusiastic about this prospect. A few are lukewarm to the idea of integrating internal controls within their entities, citing that they each “own” their part of the control structure. This stovepipe mentality continues to be a barrier to improving the integration of internal controls with an entity-wide risk management approach.

The cultural entity challenges coupled with the additional risk oversight requirements stemming from the American Recovery and Reinvestment Act of 2009 (ARRA) have made it more complicated. Together, these requirements have given many agencies the incentive and the desire to seek out a standardized process for meeting these demands.

Despite this level of ongoing risk management activity throughout the government, there has been increasing pressure on the government to do a better job at managing risks. “Recent events, like Hurricane Katrina and the subprime mortgage financial meltdown, have Americans looking to their government to ensure that these catastrophes are reduced in the future. Furthermore, the public not only demands that government manages the conse-

### Internal Controls as One Part of Enterprise Risk Management

There is some misunderstanding about the relationship between internal controls and ERM. Historically, internal controls in the federal financial management community were understood to focus on managing risks associated with financial reporting, one of many categories in the risk universe of an agency.

The underlying design of an ERM framework not only addresses risks concerning financial reporting but also intends to identify and manage all relevant areas of risks that any given agency is faced with—not just addressing the questions of compliance with the applicable controls prescribed by legislation and regulation. The value of ERM is derived from managing risk through a collective approach that enables executives to manage risk in the context of an agency’s mission, as opposed to solely focusing on an isolated piece of legislation or regulation.

quences of risk, but that it deals with problems before they turn into catastrophes. Merely reacting to risk is eroding the people’s trust in government,” wrote Charette. (Charette, 2009).

To address this issue, agencies are looking to enhance their management practices and have shown an increased interest in Enterprise Risk Management. For example, for the first time in its 75-year history, the Federal Housing Administration (FHA) announced intentions to hire its first chief risk officer. The FHA’s risk management functions are currently dispersed across a number of offices. The chief risk officer will oversee the coordination of FHA’s efforts to concentrate risk management in a single division devoted solely to managing and mitigating risk to the FHA’s insurance fund—across all FHA programs.

In addition to adding a chief risk officer, the FHA is proposing specific credit policy changes that are largely focused on ensuring responsible lending and risk management for FHA-approved lenders. These changes build on lessons learned in the credit crisis and seek to align the FHA with the administration’s goal of regulatory reform. As the FHA’s stable of lenders grows, these lenders must have “skin in the game.” These credit changes will do that by ensuring they have long-term interest in the performance of

the loans they originate. (Housing and Urban Development [HUD], 2009).

According to FHA Commissioner David H. Stevens, “given the size and scope of the FHA and its importance to today’s market, these risk management and credit policy changes are important steps in strengthening the FHA fund, by ensuring that lenders have proper and sufficient protections.” Both changes are expected to strengthen the agency’s reserves and management of risk.

In 2008, an ad hoc Federal Executive Steering Group for ERM was also established by a group of government managers from various agencies who shared a common interest in the ERM concept. This group organized the first Federal ERM Summit which brought together professionals from the private, public and educational sectors to initiate a federal dialogue. The FederalERM.com website was created to facilitate the growing interest of this topic in the federal sector.

## Examples of Risk Management in the Federal Government

Despite a lack of fundamental definitions, the discipline of risk management is not a new concept within the U.S. federal sector. It has been used in private and public sectors for decades. It is a well established practice dating back to the late 18th century, when the government began to develop policies to deal with risks thought to undermine trade and investment (Charette, 2009). “Government has always been involved in managing risks, even as risk management has not generally been recognized as being a fundamental function of government” says David Moss, a professor of business administration at the Harvard Business School. As government agencies face increased scrutiny regarding accountability, fraud, the management of resources, performance, and results, more managers are engaging in risk management activities.

Although some risk management methodologies and processes can be complex and may require expert advice and support, other aspects of risk management—such as setting goals and using performance measures to track progress in meeting them—are well understood and widely practiced (GAO, 2005). Whether the focus is on public risk, financial risk or

operational risk, agencies are managing risks that are in direct alignment with their missions or are effectively engaging the discipline as a common management practice.

### Health Risk

**Food and Drug Administration (FDA).** FDA is an agency within the Department of Health and Human Services and consists of seven centers and offices. The FDA is responsible for protecting the public health by assuring the safety, efficacy, and security of human and veterinary drugs, biological products, medical devices, our nation’s food supply, cosmetics, and products that emit radiation. The FDA is also responsible for advancing the public health by helping to speed innovations that make medicines and foods more effective, safer, and more affordable; and helping the public get the accurate, science-based information they need to use medicines and foods to improve their health.

In line with the agency’s responsibilities is the approval of medications and certain other medical products for public use and then continuous assessment of the products’ risks and benefits after they have been made available to the public (a process called post market risk surveillance). With increased attention to improving the safety and quality of health care, there has been growing interest in leveraging the large amounts of electronic health data being collected on a regular basis to enhance surveillance of post-market risk.

However, increased analytical use of personal health information raises concerns about the privacy and security of that information. According to the National Research Council, medical information is often the most privacy-sensitive information that individuals provide to others about themselves, and protecting the privacy of that information has long been recognized as an essential element in the administration of health care systems. Further, industry groups and professional associations have called for stronger protections for personal health information.

The Food and Drug Administration Amendments Act of 2007 (FDAAA) requires that FDA develop methods for the establishment of a post-market risk identification and analysis system of electronic health data. In response, FDA announced the start of its Sentinel initiative in May 2008. The initiative

includes planning for the development of an integrated system to analyze electronic health data in order to identify potential risks and assess the safety of medical products after they have been made available to the public.

### Security Risks

**Department of Defense (DoD).** The DoD uses a risk management approach to protect its forces. For example, it has used risk management to identify threats and vulnerabilities, and determine which assets are the most critical and to make management decisions on how to make its bases and related facilities more secure (GAO, 2005).

Risk management was part of the nation's approach to assessing terrorism before the events of September 11. For example, in the 1990s, the Defense Special Weapons Agency assessed risks to evaluate force protection security requirements for mass casualty terrorist incidents at military bases. Companies under contract to federal agencies such as the Department of Energy, the National Security Agency, and the National Aeronautics and Space Administration used risk assessment models and methods to identify and prioritize security requirements. The Federal Aviation Administration and the Federal Bureau of Investigation did joint threat and vulnerability assessments on airports determined to be high risk.

**Department of Homeland Security (DHS).** The threat of terrorism presents a number of risks to our nation's seaports and other types of critical infrastructure. DHS has three component agencies responsible for the security of critical infrastructure related to ports and other facilities (GAO, 2005):

- **The U.S. Coast Guard** has responsibility for port security overall. The Coast Guard is the lead federal agency for the security of the nation's ports. Its responsibilities include protecting ports, the flow of commerce, and the maritime transportation system from terrorism. As the lead in domestic maritime security, the Coast Guard has a robust presence at the national, regional, and port levels. The Coast Guard protects more than 300 ports and 95,000 miles of coastline. Coast Guard officials have been able to use expert knowledge or data from risk assessments to select specific alternatives, such as establishing security zones around key infrastructure, improving security around ferries and cruise ships, and coordinating security improvements (such as fences, gates, and cameras) around key infrastructure. Using local risk assessments, the Coast Guard has also developed alternative approaches to prevent attacks and reduce vulnerabilities.
- **The Office for Domestic Preparedness (ODP)** is responsible for providing port security grants to selected maritime facility owners. Since 2002, the program has awarded over \$500 million in grants to state, local, and industry stakeholders to improve security in and around their facilities or vessels. For fiscal year 2005, grant criteria included the prioritization of projects based on the criticality of ports and proposals that reduce vulnerabilities to certain threat scenarios. These risk-based criteria were not used in prior fiscal years.
- **The Information Analysis and Infrastructure Protection (IAIP) Directorate** is responsible for working with other federal, state, local, and private organizations to identify and protect critical infrastructure across the nation. These priorities are then to be used to direct protective measures for port security as well as across all other kinds of infrastructure. IAIP has developed a national database of critical infrastructure assets and a series of benchmark threat scenarios to be used to analyze potential attacks. IAIP has used these scenarios to develop data collection instruments for two types of assets (nuclear plants and chemical plants) to assess their vulnerabilities.

The IAIP also has a key role in applying risk management to ports and other infrastructure. Risk management is a tool for assessing risks, evaluating alternatives, making decisions, and implementing and monitoring protective measures. Relative to the Coast Guard and ODP, IAIP's homeland security responsibilities are by far the widest-ranging. The Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 (HSPD-7) charge IAIP with establishing a risk management framework across the federal government to protect the nation's critical infrastructure and key resources. The scope of this effort is immense, and the effort is one of IAIP's central responsibilities.

IAIP's task ultimately involves developing an approach that can inform decisions on what the

## The Challenge of Applying Strategic Risk Management to Homeland Security

From *Improving Strategic Risk Management at the Department of Homeland Security* by David H. Schanzer and Joe Eyerman

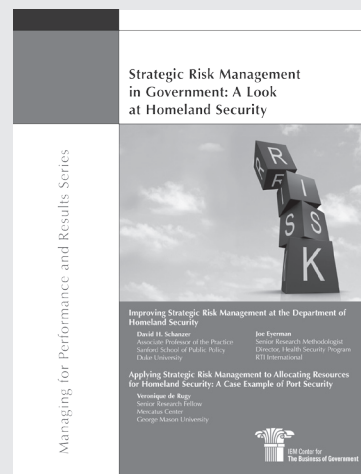
The concept of strategic risk management is not new. Businesses are constantly assessing the risks they face and taking steps to adjust to changing circumstances—whether it be selling or purchasing new assets, taking on or reducing debt, or increasing or reducing their workforce. On a micro level, families are risk managers as well. We are constantly assessing risks that we face and responding. We purchase insurance to shift certain risks to others. We take steps like fixing an old roof or getting more exercise to mitigate risks to our property or personal health. Certain risk we choose to accept—like the risk of driving to work or allowing an old tall tree to remain right next to our home. The range of choices we make in our lives are, in a sense, a form of strategic risk management.

Application of strategic risk management to the concept of homeland security, however, is relatively new and a poorly understood topic ... it was natural to turn to the field of risk science, which has been developing for decades to guide risk reduction efforts in health, the environment, transportation safety, and a variety of other areas. While there is no agreed-upon definition for the term “risk,” in its new publication, *DHS Risk Lexicon*, the department’s extended definition of risk is “potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.”

By developing tools to make mathematical calculations of these factors, risk science can provide a means of assessing the risk reduction value of a given policy, program, or budgetary investment. Even in fields where risk science is well developed, such as environmental protection, results of risk analysis are still only tools that inform decision making and cannot dictate policy results or replace the need for judgment.

Political dialogue in the years immediately following 9/11—where it appeared that every identification of a potential gap in our security led to proposals for a new program and new spending—made it clear that the government should not promise and could not deliver absolute security from terrorism. Eventually, this reality began to be reflected in the rhetoric of our political leaders, who began to speak in terms of reducing and managing risk. In April, 2002, Tom Ridge noted that “as a free and open and welcoming society, we will always be at risk. We can never totally eliminate it—but we are working every day and using every resource at our disposal to reduce it.” In 2005, this concept was adopted as the official doctrine of the Department of Homeland Security by then-Secretary Michael Chertoff, who stated, “we need to adopt a risk-based approach in both our operations and our philosophy.... [R]isk management must guide our decision making as we examine how we can best organize to prevent, respond, and recover from attack.”

“Risk management” is defined by DHS as the process by which society attempts to reduce risk “to an acceptable level at an acceptable cost.” Identifying risk management as a core principle guiding DHS activities made a great deal of sense. Yet, putting this concept into practice in the homeland security domain has proven to be a daunting task. From the earliest days after creation of the department, many placed faith in the idea that we could develop a formula or matrix that could answer the questions such as, “How much should we be spending to keep us safe?” or “Should we be spending more money on chemical detectors on subways or new anthrax vaccine?”



Strategic Risk Management  
in Government: A Look  
at Homeland Security

Managing for Performance and Results Series

Improving Strategic Risk Management at the Department of  
Homeland Security

David H. Schanzer  
Associate Professor of the Practice  
Sutton School of Public Policy  
Duke University

Joe Eyerman  
Senior Research Methodologist  
Director, Health Security Program  
RTI International

Applying Strategic Risk Management to Allocating Resources  
for Homeland Security: A Case Example of Port Security

Venugopal de Bop  
Senior Research Fellow  
Analytics Center  
Georgia Mason University



Center for the  
Business of Government



nation's antiterrorism priorities should be and identifying what strategies and programs will do the most good. More specifically, IAIP is charged with examining and comparing relative risks associated with a multitude of possible targets, ranging from specific structures (such as dams, chemical plants, and nuclear power plants) to major sectors of national infrastructure (such as the banking system, computer networks, and water systems). IAIP is also responsible for developing policies and guidance that other agencies can use in conducting their own risk assessments.

The application of risk management in homeland security is relatively new—much of it coming in the wake of the terrorist attacks of September 11—and it is a difficult task with little precedent. The goals for using it in homeland security include informing strategic decisions on ways to reduce the likelihood that adverse events will occur, and mitigate the negative impacts of and ensure a speedy recovery from those that do. Achieving these goals involves making policy decisions about what the nation's homeland security priorities should be—for example what the relative security priorities should be among seaports, airports, and rail—and basing spending decisions on what approaches or strategies will do the most good at narrowing the security gaps that exist. Risk management has been widely supported by the president and Congress as a management approach for homeland security, and the secretary of the Department of Homeland Security has made it the centerpiece of agency policy.

## Financial Risks

**Government National Mortgage Association (GNMA).** GNMA or “Ginnie Mae”, is a wholly owned corporation housed within the Department of Housing and Urban Development. For nearly four decades, GNMA has made financial risk management one of its core values. This has allowed it to keep pace with, and frequently surpass, private sector financial risk management practices.

The primary mission for GNMA is to “support expanded affordable housing in America by providing an efficient government-guaranteed secondary market vehicle linking the capital markets with federal housing markets.” This is accomplished with fewer than 100 employees and under the leadership of a strong management team. In 2008, the corpora-

tion celebrated 40 years of “financial stability.” GNMA undoubtedly has a mission closer to private sector organizations than many government agencies, yet it has a subtle but important distinction: Its primary purpose is to support and expand the market for affordable housing, *not to maximize profits*. FHA loans in particular are typically made to borrowers that would have difficulty getting loans under normal private sector programs. The general perception is that these loans have higher delinquency and default rates than their conventional counterparts. Because of this, Congress was concerned that private sector secondary market participants would not be willing to bear this risk, and so it created GNMA to ensure that such a market existed.

Historically the mission of GNMA has meant ensuring the existence of a secondary market for FHA/VA-insured mortgages, and GNMA has created an innovative system to meet this mission. GNMA does this by guaranteeing the performance of the issuers of Mortgage Backed Securities (MBS). The issuers form these MBS's from pools of FHA and VA mortgage loans.

GNMA does not insure individual mortgage loans; that is the mission of FHA or VA insurance and of the MBS issuer. Rather what it does do is guarantee that if the issuer of the MBS goes into default—i.e., does not make their promised payments to the investors—the investors are still paid. The mission and operations of GNMA illustrate one of the most important points about risk in general: Managing financial risk does not mean eliminating it. In fact, in the case of GNMA this would be virtually impossible; as long as it is operating, it must take on financial risk. What GNMA must do is balance the risk that it takes against the accomplishment of its mission. The only way for GNMA to eliminate all of its financial risk is to not insure any issuers. The key for GNMA is to maximize its mission accomplishment while minimizing the financial risk that it bears (Buttimer, 2001).

## Transportation Safety Risks

**National Transportation Safety Board (NTSB).** The NTSB is an independent federal agency charged by Congress with investigating every civil aviation accident in the United States and significant accidents in the other modes of transportation—railroad, highway, marine, and pipeline—and issuing safety recommendations aimed at preventing future accidents.

The Safety Board determines the probable cause of:

- All U.S. civil aviation accidents and certain public-use aircraft accidents
- Selected highway accidents
- Railroad accidents involving passenger trains or any train accident that results in at least one fatality or major property damage
- Major marine accidents and any marine accident involving a public and a nonpublic vessel
- Pipeline accidents involving a fatality or substantial property damage
- Releases of hazardous materials in all forms of transportation
- Selected transportation accidents that involve problems of a recurring nature

The NTSB has made great strides in mitigating the results of accidents and is now concentrating on prevention (Charette, 2009). A seemingly unlikely goal for an agency whose primary objective is to investigate accidents after they occur, the NTSB has invested in this emerging area. One accomplishment has been the development of guidelines to help reduce travel-related risks, which in the case of car crashes, take the lives of 40,000 people and injure 3 million others every year.

Over the last four decades, NTSB has investigated 124,000 aviation accidents and 10,000 crashes involving trains, ships, trucks, and cars. The Board has also found a way to leverage existing products, such as the issuance of safety recommendations after investigations, to help offset and reduce the public's risk when flying, driving, boating, and traveling by rail.

One compelling linkage of risk to mission is the NTSB's creation of the Most Wanted List. Created in 1990, this list includes dozens of suggestions on how to make travel safer. The list has been credited with reducing transportation risks.

### External Risks

**United States Postal Service (USPS).** Managing risk certainly isn't new to the USPS. The mission of the service is to provide trusted, reliable, affordable universal service. Each day, the service delivers to 150 million U.S. addresses and countless more worldwide. The service also helps customers build and

### Neither rain, nor sleet, nor dark of night... "Nor epidemic?"

The USPS has also been proactively participating in managing a shared public risk not affiliated with the everyday delivery of postal services. In 2004, USPS announced that it could be called upon to deliver antibiotics from the Strategic National Stockpile directly to residential addresses in the event of a catastrophic incident involving a biological agent for which antibiotic use was appropriate.

In 2005, USPS signed the National Response Plan, which was developed by the U.S. Department of Homeland Security. The National Response Plan established a standardized approach for all levels of government to work together, to protect citizens and manage homeland security incidents. All federal departments and agencies that assist during a national incident will use this plan, whether from threats or acts of terrorism, major natural disasters, or man-made emergencies.

In 2009, a world epidemic of the H1N1 virus (Swine Flu) spread from Mexico City to other countries such as Europe and the United States in record numbers, challenging our way of life. The USPS's preparation for responding to this emergency prior to the 2009 flu incident is the type of leadership citizens are looking for from their government when managing risks.

maintain relationships, share sensitive information, and exchange goods and services. From 2001 to 2005, USPS came face to face with a series of events that impacted its operations. This included September 11 and the anthrax response in 2001, the New York City blackout and West Coast wildfires in 2003, and Hurricane Katrina in 2005. For the USPS, on-time delivery is the critical first step in meeting and satisfying postal customer needs. Yet, despite the events between 2004–2005, the USPS continued the trend of steadily improving performance, achieving its highest score ever for the delivery of single-piece first-class mail.

USPS has done a good job of managing external risks to ensure minimum disruption to services. However, its biggest challenges and threats to continued success lay in the realm of its internal business operations.

Long-term, the service is facing major operational hurdles that are forcing the organization to reconsider

how it manages strategic, financial, and operational risks. For instance, electronic diversion and a tough economic climate continue to reduce volume and revenue. Fortunately, many of its costs—such as a carrier’s daily stop at every address—are fixed, regardless of volume and are manageable. Other costs, such as energy and benefits, are rising faster than inflation while prices for 90 percent of its revenue base are capped at the rate of inflation. The growing revenue/cost gap is a serious threat to the service’s ability to provide affordable universal service, an essential element of its core mission. USPS leadership is cognizant of the reality that the severity of the situation and the pace of change demand an agile, flexible organization. To address these issues, USPS has established Vision 2013, the organization’s five-year strategic plan for building its business and sustaining a strong, viable Postal Service during turbulent times.

### Operational Risks

**Internal Revenue Service (IRS).** For nearly 60 years, the IRS has fulfilled its purpose of collecting federal taxes—\$1.7 trillion worth to be exact, which is more than 26 times its collections in 1952. Over the last 57 years, the volume and complexity of IRS operations expanded tremendously. The number of returns filed has more than doubled, the number of pages in the tax code has expanded from 812 to approximately 3,500, and approximately 9,500 changes to the tax code were made. The IRS employs 80,000 full-time and 10,000 seasonal and part-time employees and has a FY2009 budget of nearly \$12 billion.

The IRS today deals directly with more Americans than any other institution, private or public. To keep pace with the exponential growth over the last decades, the agency sought to update its infrastructure and operations to better serve the American taxpayers. The IRS Restructuring and Reform Act of 1998 (RRA ‘98), which passed with bipartisan support, incorporated many of the recommendations found in studies conducted to pinpoint areas of improvement. The RRA prompted the most comprehensive reorganization and modernization of IRS in nearly half a century. The IRS reorganized itself to closely resemble the private sector model of organizing around customers with similar needs.

As required by the RRA ‘98, this direction is expressed in the new IRS mission statement:

“Provide America’s taxpayers top quality service by helping them understand and meet their tax responsibilities and by applying the tax law with integrity and fairness to all.”

It is the role of the IRS to help the large majority of taxpayers who are willing to comply with the tax law, while seeing to it that the minority who are not willing to comply are not a burden to fellow taxpayers. The IRS must perform this role to a top quality standard, which means that all of its services should be seen by the people who receive them as comparable in quality to the best they get elsewhere.

However, achieving this mission requires fundamental change in many aspects of an institution that has been built over many years. This change must produce success in the new mission, while retaining the essential elements that created success in the past. Further, this change must take place while the IRS continues to administer a very large, complex and ever-changing tax system.

As outlined in the IRS Organization Blueprint (IRS, 2000), the whole process of change is referred to as “modernization” because it involves building on the essential components that made the IRS successful in the past while bringing it up to date in a way designed to achieve the new mission. In the agency’s Blueprint, modernization at the IRS has required change on five major fronts:

- Revamping business practices
- Establishing customer-focused operating divisions
- Creating management roles with clear accountability
- Instituting a balanced performance measurement system
- Overhauling the entire technology base

Since 2000, the agency has also included human capital challenges.

### *The Risks of Modernization*

The amount of change required for modernization, coupled with current complex operations, means that there is significant risk that unanticipated problems will arise, and operational errors will occur. In addition, the information technology on which the

IRS critically depends is fragile and deficient and cannot be fixed short of a near total replacement. Yet, success in modernization of technology can only be achieved with the appropriate management and organization structure and a program to modernize business practices. Although there are inherent risks in the modernization process, knowing that they exist means that they can be managed and mitigated so that no setback is fatal (IRS, 2000).

Like many organizations, the IRS faces the challenge of managing and absorbing change. These limitations arise from such things as the capacity of the top managers to understand, plan, and make correct decisions about the many complex issues that arise and the capacity of managers and employees throughout the organization to learn many new ways of doing business. Capacity to make change rapidly is further limited by the need to ensure that essential services, such as the filing season, are never jeopardized and the financial integrity of the revenue stream is maintained. The inherent limitations of organizational capacity and the need to manage risk make it essential to set overall priorities in light of the overall goals.

**ERM Drivers at IRS**

The nature and complexity of both the reorganization and the modernization was a major segue for the IRS to identify and mitigate structural, technological and operational risks where and when possible. But as with many agencies, these risks were frequently compartmentalized and addressed within the individual organizational segments creating a fragmentation in the governance, risk management, and compliance structure. The mere presence of risk does not necessarily translate into a culture of risk management.

However, the opportunity to integrate risk management through ERM evolved out of necessity, as with most agencies. Usually, if top leadership does not have a passion for ERM, the agency will not have a risk-based focus. “When the initial interest in ERM does not come from the top, it can be inspired from the bottom-up or vertically from across the organization,” says Hess. This is the case with the IRS.

The Office of Program Evaluation & Risk Analysis (OPERA), which is part of IRS’s Research Program, is the sponsoring organization within the IRS for advocating a standard ERM process. A critical component of OPERA’s mission is to promote risk management within the IRS. Since its inception ten years ago, OPERA has worked with strategic planning, modernization and other IRS programs to leverage risk management with existing processes. Most recently, OPERA has worked with the modernization program to develop options for a risk framework for evaluating strategies for reaching a successful “end state.” In past years, OPERA identified enterprise risks through its strategic planning and budgeting processes to facilitate risk-based decision-making around key organizational issues.

While the modernization project is one driver of ERM at the IRS, OPERA has identified others (see Table 1).

**The IRS Risk Profile**

Without a proper understanding of an organization’s internal environment and orientation towards risks it would be difficult to integrate a risk management process within its business operations. Thus, developing a risk management profile will provide leaders with the insight needed to understand the different risks that apply to their organization and serve as the foundation for long-term strategic planning surrounding key risks.

**Table 1: ERM Drivers at the IRS**

External Drivers	Internal Drivers
<ul style="list-style-type: none"> <li>• Advancing Technology (e-filing, web-based services)</li> <li>• Implementing regulations (Sarbanes-Oxley requirements, immigration, pay for performance)</li> <li>• Monitoring threats (terrorism, natural disasters) to business operations</li> <li>• Responding to oversight (GAO, OMB) to better manage IRS’s risk portfolio</li> </ul>	<ul style="list-style-type: none"> <li>• Understanding strategic and operational risks</li> <li>• Improving coordination and decision-making around risks</li> <li>• Increasing ability to identify, quantify, measure, and monitor cross-cutting risks</li> <li>• Ensuring that existing structures and processes are considered in decision-making</li> <li>• Addressing operational risks</li> </ul>

Source: Hess, 2007

Agencies have a better chance of successfully implementing ERM if they:

- Know how much risk the organization can tolerate (*risk appetite*)
- Recognize the organization's strengths and weaknesses in managing risks (*risk maturity*)
- Know how an organization treats a risk once identified (*risk response*)

For example, in terms of risk appetite, the IRS is a conservative, risk averse organization that responds well to problems, once known. IRS's successful responses to recent stimulus payments and annual tax law changes are two such examples. However, IRS does not consistently apply risk management disciplines strategically or at an enterprise level. The IRS has established mechanisms to respond to and manage risks (e.g., executive steering committees and business continuity plans), and there are ERM practices applied in the organization, but not in an integrated manner. There are numerous governance structures in place for the agency, such as the Human Capital Board, Enforcement Committee, Strategy and Resource Committee, and Filing Season Readiness. But there is no specific governing body established with a mixed representation of agency leadership to view a portfolio of agency risks. This may be one of the weaknesses of the ERM effort at the IRS.

As for maturation, risk management is decentralized and usually not explicitly referred to or understood as risk management. "Inherently, staff are thinking and doing risk management, but it is not called risk management," says Christopher Hess of OPERA. "But people still see risk as a consequence rather than an opportunity to improve and as another task added to their plate."

This is not a unique barrier for the IRS and is quite common within other federal agencies attempting to implement ERM. OPERA has worked diligently to diffuse this perception by raising awareness of ERM through workshops, briefings, and internal/external information sharing. "Last year we conducted a one day ERM seminar that included employees from both the operating divisions and support functions. The objective was to obtain employee input on how ERM could best be developed within the IRS. The initial feedback was positive," says Hess. OPERA has also used the strategic planning process as a vehicle for

introducing ERM disciplines and practices, identified cross-cutting risks through annual corporate strategic analyses, and conducted case studies to identify areas internally where ERM disciplines are practiced.

To further develop ERM at the IRS, the agency is building on critical business analyses, studying other public and private sector organizations with comparable risk identification processes, and beginning to consider incentives to encourage risk identification. For all of the progress made since introducing the ERM concept in 2007, the process is still in the development stage. "For now each organization within the IRS continues to use their own approach and methodology for managing risk. It is our goal to mature the process over time," says Hess.

# Applying Risk Management in Government: Centers for Disease Control and Prevention

The mission of the Centers for Disease Control and Prevention (CDC) is to promote health and quality of life by preventing and controlling disease, injury, and disability. The CDC was selected as a case study because of the agency's experience in Issues Management and how it is integrated into the agency's ERM efforts.

CDC seeks to accomplish its mission by working with partners throughout the nation and the world to:

- Monitor health
- Detect and investigate health problems
- Conduct research to enhance prevention
- Develop and advocate sound public health policies
- Implement prevention strategies
- Promote healthy behaviors
- Foster safe and healthful environments
- Provide leadership and training

Those functions are the backbone of CDC's mission. Each of CDC's component organizations undertakes these activities in conducting its specific programs. The steps needed to accomplish this mission are also based on scientific excellence, requiring well-trained public health practitioners and leaders dedicated to high standards of quality and ethical practice.

CDC operates in accordance to three core values, *Accountability*, *Respect*, and *Integrity*, and pledges to:

- Be a diligent steward of the funds entrusted to it
- Provide an environment for intellectual and personal growth and integrity

## CDC's Core Values

**Accountability:** As diligent stewards of public trust and public funds, we act decisively and compassionately in service to the people's health. We ensure that our research and our services are based on sound science and meet real public needs to achieve our public health goals.

**Respect:** We respect and understand our interdependence with all people, both inside the agency and throughout the world, treating them and their contributions with dignity and valuing individual and cultural diversity. We are committed to achieving a diverse workforce at all levels of the organization.

**Integrity:** We are honest and ethical in all we do. We will do what we say. We prize scientific integrity and professional excellence.

**Source:** CDC website at <http://www.cdc.gov/about/organization/mission.htm>

- Base all public health decisions on the highest quality scientific data, openly and objectively derived
- Place the benefits to society above the benefits to the institution
- Treat all persons with dignity, honesty, and respect

## CDC Approach to ERM

Leadership at the CDC established a holistic risk recognition and mitigation process comprising three key components:

- ERM
- Issues management
- Credibility risk management

## ERM

The first leg of the tripod involves the adoption of ERM. Established in September 2005, the Office of Enterprise Communication (OEC) reports directly to the CDC Director and is responsible for coordinating the agency's response to urgent issues and ensuring consistent communication to key CDC issues, both internally and externally. This includes managing the agency's risk recognition and mitigation process. CDC's philosophy regarding ERM is indicative of the various ways this process is being applied across agencies. For the CDC, "risk" is defined as the potential harm that may arise from some present process or from some future event. ERM at the CDC is defined as "the process of analyzing the organization's exposure to risk and determining how to best handle such exposure."

The core principles behind CDC's approach to ERM include a willingness to review policies and practices to find vulnerabilities and opportunities to ask the question "What if?" The agency stresses that when they find vulnerabilities there must be an effort to change policies and practices to reduce risk. The agency is moving forward with a professional and systematic approach that requires buy-in. This involves briefing executive leadership on the types of risks facing the agency, providing a framework for discussing risk recognition and mitigation, and recruiting leadership to support CDC's RiskSmart™ credibility risk management and issues management systems.

For the CDC, selling ERM to senior leadership also included outlining the following universal steps in risk management:

- Establish the context for enterprise risk management
- Identify risks
- Analyze risks
- Treat risks

This process mirrors that of the COSO Enterprise Risk Management framework and the Canadian Integrated Risk Management framework.

As a bottom-up strategy for assessing risk, the CDC Internal Controls Program feeds into and supports the broader, top-down approach to ERM. This program is managed by the organization's Management

and Analysis Services Office (MASO) and keeps track of the inventory of risks that need to be reviewed on a cyclical basis. MASO oversees the fulfillment of requirements set forth in the Federal Manager's Financial Integrity Act (FMFIA). MASO's mission is fully integrated with FMFIA internal control OMB Circular A-123 Appendix A activities and represents a collaborative effort between financial and administrative managers. As a non-voting entity of the CDC's Risk and Resilience Standing Committee, a subgroup of the agency's Executive Leadership Board, MASO contributes a financial and analytical perspective to the Credibility risk analysis process.

MASO also works with senior management to identify transactions cycles to be reviewed at operating division levels. For example, in one cycle year, the CDC conducted 235 risk assessments and completed in-depth reviews of 41 assessable units (in 67 separate reviews). Twenty-one of those assessable units reviewed supported the reporting requirements under A-123 Appendix A activities. The primary review categories under the Internal Controls Program are common throughout the federal government which includes procurement, human capital management, financial reporting, grants management, information technology, disaster relief, and budget/spending plans.

The employment of the ERM concept at the executive level leverages an already mature internal controls program by adding a stronger and more holistic governance structure to the process. The ERM effort also increases accountability at the management level, reinforces the need to eliminate stovepipes, and embraces cross-collaboration between agency functions. These are reflective of the common themes emerging from the practices of ERM agency leaders involved in the implementation process of risk management.

## Issues Management

According to the Issues Management Council, "issues management" is the process of prioritizing and proactively addressing public health reputation issues that can affect the organization's success. The operating definition used by the CDC positions issue management as "the process of prioritizing and proactively addressing public policy and reputation issues that can affect an organization's success." CDC's Issue Management system feeds into the

agency's ERM model, alerting management to issues that could become bigger problems.

"The basic research, analytical and logistical components are in place throughout the Agency to foster the development and implementation of an effective issues management system at CDC," says Donna Garland, Director, Office of Enterprise Communication. The existence of staff within the Office of the Director that unifies professionals trained to handle risk communications and issues management is a historic milestone for CDC. This management construct is further enhanced by a streamlined communications system that places enterprise communication officers in each coordinating center, a strategy that provides direct information sharing to the OEC. Not only does this unify the expertise of public affairs professionals; it also creates a "natural foundation which the CDC RiskSmart™ issues management system can be developed and implemented in the future."

### Credibility Risk Management

For the CDC, credibility is high priority. Agency leaders believe that how they communicate as an organization should actively be informed by how they are being perceived. To some extent, CDC has taken into consideration the wisdom of Warren Buffet, who said "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." This may describe the spirit behind CDC's ERM effort in doing things differently when it pertains to maintaining and sustaining their reputation for promoting health and quality of life.

"Reputation" is the perception held by interested persons or groups about the agency's characteristics, achievements, and behaviors. From the CDC's perspective, managing the agency's reputation is important because the agency must have the public's trust to do its mission, or risk:

- Increased disease, injury and death
- Demands for the misallocation of limited resources
- Circumvented public health policies

"Credibility is about establishing and consistently maintaining the trust of stakeholders. The position the agency is taking and establishing is that an orga-

### How the CDC Measures Credibility Risk: RiskSmart™

The CDC feels so strongly about its reputation that it has developed and proposed a separate risk assessment strategy to measure credibility. The tool, referred to as RiskSmart™ or *Credibility Risk Management*, is an active, continuous, and ethics-based assessment and engagement with all stakeholders to safeguard and enhance the agency's credibility.

According to the Canadian Integrated Risk Management Framework, a "risk-smart" workforce and environment in the public service is one that supports responsible risk management, where risk management is built into existing governance and organizational structures, and planning and operational processes. An essential element of a risk-smart environment is to ensure that the workplace has the capacity and tools to be innovative while recognizing and respecting the need to be prudent in protecting the public interest and maintaining public trust.

To that end, the CDC RiskSmart™ system is a toolkit with three components: the RiskSmart™ Signal environmental scanning tool; the RiskSmart™ Assessment Tool, and the Burkean Pentad. The RiskSmart™ system is also composed of three basic activities:

- **Credibility Enhancement:** measure, preserve, and grow stakeholder trust
- **Credibility Risk Mitigation:** monitor, detect, assess, forestall or respond to threats to stakeholder trust.
- **SWOT Analysis:** Assessing agency Strengths, Weaknesses, Opportunities, and Threats

CDC utilizes the RiskSmart™ Signal, an environmental scanning tool for detecting credibility risks. It is a streamlined tool that can be used throughout the agency to detect credibility risks more quickly and systematically. With this tool, CDC can detect risks early. Once the potential credibility risk is detected, a more in-depth, multi-faceted assessment of the risk is conducted using the CDC RiskSmart™ Assessment Tool. The tool "helps to make the risk identification and assessment process less overwhelming and it minimizes discretions in the risk assessment process," says Donna Garland.



nization holds the trust of its publics by being truthful, stalwart in the face of challenges, and [engaging in strategic risk-taking that leads to innovation],” says Garland. Indeed, a part of the change that has to take place regarding perceptions of risk is the ability to associate innovation, and not just consequence with risk as mentioned earlier in the report. “If issues are well managed—navigating negative ones well and maximizing positive ones—you will stabilize or improve your credibility,” says Garland. “If, however, issues are poorly managed your current credibility is damaged and future credibility can be hurt as stakeholders question your ability to be effective.”

Conceptually, CDC likens its reputation (everything they do and how they communicate about what they do) to the double helix of DNA—that is to say, both are intertwined. “The building block of everything that makes up [an agency’s] identity is expressed by the accumulation of individual events strung together. Like the DNA’s double helix, activities that enhance or protect the brand can’t be separated. It is the agency’s collective behavior and communication that determines its success.”

## Key Drivers of ERM at CDC

The CDC identifies maintaining high agency credibility (or its reputation) as the primary driver for implementing ERM. All agencies have this intangible asset, but arguably, few emphasize its importance. Other organizations also share this endeavor. Industry experts note that intangible assets such as brand equity and goodwill account for 70%-80% of a company’s market value. Yet, most companies don’t proactively manage reputation risk until after their reputation suffers damage (Eccles, Newquist & Schatz, 2009). Even though government agencies are not assessed according to market value, the perceptions of taxpayers, the general public and political governing bodies have as much impact just the same.

As described in the article “Reputation and Its Risks” published in the *Harvard Business Review* “most companies do an inadequate job of managing their reputations and the risks to their reputations in particular. They tend to focus their energies on handling the threats to their reputations that have already surfaced. This is not risk management; it is crisis management—a reactive approach whose purpose is to limit the damage.” (Eccles, Scott and Schatz, 2009)

## ERM Governance Structure at CDC

The CDC models its ERM governance structure after that of the Department of Health and Human Services (DHHS) structure for overseeing the FMFIA process. The DHHS issues on an annual basis an OMB Circular A-123 guidance manual for its 12 operating divisions and requires each organization to establish its own Senior Assessment Team (or other governance body) to conduct and oversee the day-to-day activities of the OPDIV internal control and financial systems assessment processes. The CDC surpassed that objective by establishing a two-tiered governance structure that would also provide oversight of the ERM process.

The Executive Leadership Board (ELB) serves as the governance structure for the entire agency. The Risk and Resilience Executive Leadership Standing Committee (RRSC) is chartered by and a sub-component of the ELB. The RRSC is a 12-member committee accountable for developing a sustainable enterprise risk management program to help ensure that the CDC effectively carries out its mission, meets its goals, and maintains public trust. Members reflect a cross-representation of subject-matter expertise and leadership across the agency with a range of thinking styles to enable broad issue analysis. The membership was devised to cover areas of potential external and internal risk. All the members have been educated about ERM and are asked to sit at the table and think with an “agency” perspective.

The RRSC recommends strategic actions to prevent or reduce the risk or their harmful consequences to the agency and improve the agency’s overall resilience. In addition to providing timely and pre-decisional analysis to support evidence-based decision making by the ELB, the RRSC provides guidance and counsel to CDC, through the ELB, regarding specific enterprise risk questions, issues, and topics. To help manage the “white spaces” within the organization, the RRSC also engages with key CDC scientific, program, and management staff to discuss risk prevention and mitigation strategies.

# Applying Risk Management in Government: Department of Education

The mission of the U.S. Department of Education (ED) is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access. The Department of Education was selected as a case study because of its use of ERM to respond to the high risks identified in Federal Student Aid.

ED's 4,300 employees and \$68.6 billion budget are dedicated to:

- Establishing policies on federal financial aid for education, and distributing as well as monitoring those funds
- Collecting data on America's schools and disseminating research
- Focusing national attention on key educational issues
- Prohibiting discrimination and ensuring equal access to education

Education is a national priority. ED is the primary agency responsible for overseeing the investment of the federal government support of U.S. education. The Department is committed to giving students the skills they need to succeed in a highly competitive global economy. To this end, it has established goals to address the following three priorities:

- Increase student achievement, reward qualified teachers, and renew troubled schools so that every student can read and do math at grade level by 2014, as called for by *No Child Left Behind*
- Encourage more rigorous and advanced coursework to improve the academic performance of our middle and high school students

- Work with colleges and universities to improve access, affordability, and accountability

## Federal Student Aid

Federal Student Aid (FSA), the largest principal office of the U.S. Department of Education, seeks to ensure that all eligible individuals can benefit from federally funded or federally guaranteed financial assistance for education beyond high school. Federal Student Aid works with postsecondary schools, financial institutions and other participants in the Title IV student financial assistance programs to deliver programs and services that student finance their education beyond high school. Federal Student Aid is responsible for a range of critical functions that include, among others:

- Processing millions of student financial aid applications
- Disbursing billions of dollars in aid funds to students through schools
- Enforcing financial aid rules and regulations
- Educating students and families on the process of obtaining aid and other college funding
- Servicing millions of student loan accounts
- Securing repayment from borrowers who have defaulted on their loans
- Operating information technology systems and tools that help manage our billions in student aid dollars

The 1998 reauthorization of the Higher Education Act (HEA) established Federal Student Aid as a performance-based organization (PBO), to administer student financial assistance programs under Title IV of the HEA at the U.S. Department of Education.

**Excerpt from  
Department of Education Strategies  
2007–2012**

**Cross-Goal Objective: Maintain and strengthen financial integrity and management and internal controls.** The Department must be a high-performing organization internally to achieve its national policy goals. From now through FY2012, the Department will build upon a series of clean audit opinions to sustain high-quality financial oversight and identify and reduce risk in internal management activities. Achievement of targets for performance measures will engender trust among Americans in the integrity of the Department's financial activities, support informed management and policy decision-making, and help achieve the broader goal of leaving no child behind.

**Strategy: Implement risk mitigation activities to strengthen internal control and the quality of information used by managers.** Beginning in FY 2007, the Department began to build a database comprising internal controls and potential program and administrative risks. The Department's principal offices will track their progress on various risk management components, making it possible to identify and correct problems quickly. Enhanced business intelligence will lead to better management decisions, improved cost efficiencies, and more rigorous internal controls.

Pursuant to the PBO legislation, Federal Student Aid is led by a chief operating officer, who advises the secretary on Department matters related to the administration and oversight of student financial assistance programs. These financial aid programs (Title IV programs), include Pell Grants, Stafford Loans, PLUS Loans, and the "campus-based" programs: Federal Work Study, Perkins Loans, and Federal Supplemental Educational Opportunity Grants. In fiscal year 2008, Federal Student Aid operated on an annual administrative budget of approximately \$629 million.

**Key Drivers for Enterprise Risk Management (ERM) at FSA**

In 1990, GAO placed the student financial aid programs on its high-risk list for fraud, waste, abuse, or mismanagement, "citing the lack of financial and management information needed to manage these programs effectively and the internal controls needed to maintain the integrity of their operations."

In an effort to address findings and weaknesses cited by GAO, ED took various actions to provide support for removal of the student financial assistance programs from GAO's High-Risk list.

In 2001, the Government Accountability Office (GAO) in its Performance and Accountability Series report outlined several major management challenges and program risks at the Department of Education. One major challenge focused on the Office of Student Financial Assistance's (FSA's predecessor) ability to ensure access to postsecondary education while reducing the vulnerability of student aid programs to fraud, waste, error, and mismanagement. The federal loan and grant programs administered by Federal Student Aid help finance the higher education of millions of students. Annually, these programs provide billions of dollars in federal loans and grants.

In its 2001 report, GAO noted that while these programs have been successful in providing students with access to money for postsecondary education, they had been less successful in protecting the financial interests of the federal government and U.S. taxpayers. Specifically, the GAO reported that although the student loan default rate had declined to 6.9 percent in fiscal year 1998, student loan defaults still cost the federal government billions of dollars each year—\$4.3 billion in fiscal year 1999 alone and more than \$28 billion the 10 years between 1991 and 2001. In addition, GAO cited that with the exception of fiscal year 1997, Education had not received an unqualified—or "clean"—opinion on its financial statements since its first agency-wide audit in 1995.

In 2002, the secretary of Education made removal from GAO's High-Risk list a specific goal and listed it as a performance measure in Education's strategic plan. In response to this goal, FSA undertook several key initiatives to address concerns about systems integration, defaulted loan reporting, and human capital management. In its 2005 High-Risk update, GAO reported that ED had "demonstrated a strong commitment to addressing risks; developed and implemented corrective action plans, and through its annual planning and reporting processes, monitored the effectiveness and sustainability of its corrective measures" and removed the student financial aid programs from its High Risk list.

**FSA’s Risk Management Efforts**

The Department’s goal of strengthening financial integrity and internal controls was the primary driver behind FSA’s decision to establish an enterprise risk management organization and in the hiring of FSA’s first chief risk officer (CRO). 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.

As the first CRO, Stan Dore led the effort to develop and prioritize activities for establishing and implementing an ERM vision, strategy and framework at FSA. With extensive financial, audit and risk management expertise, Dore brought more than 20 years of experience in the banking and financial services industries to FSA and was able to articulate an ERM vision for the agency’s leaders regarding the process, context and value of ERM.

Since most federal agency efforts relating to risk have been limited to focus on financial controls and A-123 activities, Dore, like other ERM champions in the federal sector, faced limited availability of ERM guidance, best practices, or other strategic approaches for identifying, assessing and managing risk at government agencies. Despite these challenges, FSA moved forward with establishing a foundation for implementing its own ERM program. A few of the

initial efforts associated with that effort have included:

- Establishing the FSA’s Enterprise Risk Management Group (ERMG)
- Establishing an ERM committee and charter
- Creating an ERM strategy and developing process for implementing a COSO-based ERM Framework

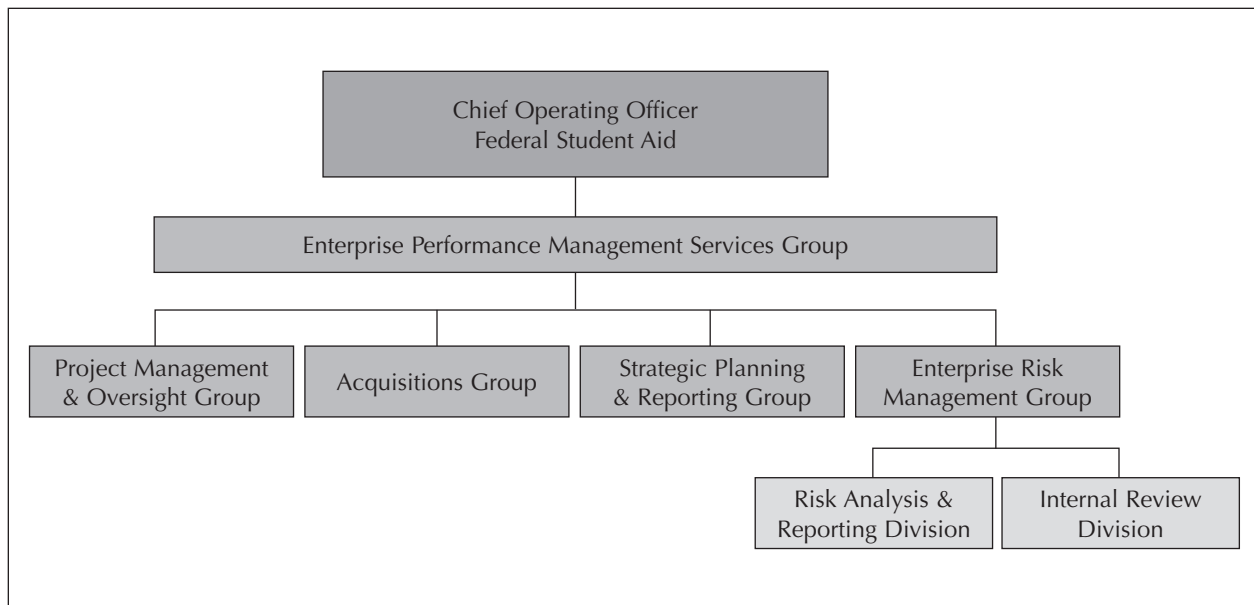
In 2006, the ERMG began efforts to implement a COSO-based ERM framework.

**FSA’s Enterprise Risk Management Organization**

The mission of FSA’s Enterprise Risk Management Group (ERMG) is to enhance the ability of Federal Student Aid to identify, assess, and manage risk across the enterprise. In support of that mission, ERMG provides risk management oversight and guidance to Federal Student Aid and performs internal reviews and risk assessments as appropriate or as requested by senior management. ERMG drives strategies and plans for assessing, monitoring and addressing risk associated with Federal Student Aid, its programs, systems, contracts, and external partners.

Audit tracking and resolution is also a priority. FSA partnered with the OIG on joint fraud initiatives to identify and reduce fraud associated with the administration of Title IV programs. This initiative

**Figure 1: FSA Organizational Chart**



involves a team approach focusing on assessing and quantifying risk and exposure associated with specific fraud issues or areas or programs more susceptible to fraud or abuse.

To accomplish its overall mission, ERMG is organized into two main areas: Risk Analysis & Reporting Division and Internal Review Division.

### ***Risk Analysis & Reporting Division***

The Risk Analysis & Reporting Division is responsible for providing enterprise-wide risk management oversight and guidance and has the following goals, objectives and responsibilities:

- Improving risk management efforts, activities and reporting
- Coordinating annual high-level risk assessments of Federal Student Aid
- Performing targeted risk assessments at the direction of senior management or as deemed appropriate
- Implementing data analysis techniques and risk assessment methodologies to improve efforts to quantify, evaluate and report on risk
- Assisting in the review, evaluation and approval of key projects, systems and organizational changes
- Developing an enterprise risk management strategy
- Establishing and implementing an enterprise risk management framework

### ***Internal Review Division***

The Internal Review Division is responsible for helping to ensure that an effective internal control framework is in place across the enterprise and has the following goals, objectives and responsibilities:

- Monitoring Federal Student Aid's performance in high-risk areas identified by the Government Accountability Office (GAO)
- Coordinating meetings with GAO on high-risk issues
- Serving as Federal Student Aid's official audit liaison with authority delegated from the chief operating officer
- Reporting on audit exception/resolution progress

- Reporting on status of Corrective Action Plans execution
- Working with Education's Office of Inspector General and GAO to facilitate their audits and address identified issues
- Assisting in the review, evaluation and approval of key projects, systems and organizational changes
- Performing internal reviews at the direction of senior management

## **The ERM Governance Structure**

Support for ERMG and the organization's ERM programs comes first and foremost from the head of Federal Student Aid: FSA's chief operating officer (COO). While the CRO reports administratively to the general manager of Enterprise Performance Management Services, he has a 'dotted line' relationship to COO and meets regularly with the COO to discuss risk management and internal review issues facing the organization.

FSA has established an ERM committee consistent with the roles and responsibilities identified in the COSO framework. The ERM Committee is comprised of five executives:

- Chief financial officer
- Chief information officer
- Chief business operations officer
- Chief of staff to the chief operating officer
- Chief risk officer

The purpose of the ERM committee is to assist the chief operating officer in:

- Assessing and evaluating major (strategic) risks
- Establishing the organization's risk profile and setting risk tolerances
- Reviewing and approving Federal Student Aid's ERM strategy
- Monitoring the implementation of FSA's ERM Program and framework

Since FSA's ERM committee is a subset of the organization's Executive Leadership Team (ELT), which plays a primary role in key decisions around strategy, risk and allocation of resources, the role of the ERM committee is sometimes handled by the ELT. Therefore,

as FSA's ERM program continues to evolve, the role and composition of the ERM committee is being reevaluated to ensure proper fit within FSA's executive management structure.

### **ERM Program Strategy & Methodology**

Federal Student Aid's ERM strategy calls for implementing program activities in several phases. These activities support two approaches that are designed to collectively achieve the objectives of the ERM program. The "top-down" approach represents a high-level effort to identify and evaluate the top risks facing the organization, focusing on those risks that could prevent the organization from achieving its stated strategic objectives.

The "bottom-up" approach refers to the conduct of various business unit risk activities using a COSO-based ERM Framework adopted by FSA. The initial risk activities center around the development and population of an enterprise risk database, and includes the identification, classification, and assessment of risks in each of FSA's approximately 27 business units, with a focus on those risks that could affect each area's ability to achieve its organizational goals and objectives. As part of this effort, the identified risks are being documented, categorized and assigned risk ratings, so that each risk can be ranked according to its significance, likelihood, or other criteria, with more significant, enterprise and/or strategic risks flowing up to senior management and presented in a portfolio view.

Additional efforts underway associated with the "bottom-up" approach include: the development of a methodology to evaluate risk response strategies and control activities; various activities designed to provide for enhanced risk information and improved communication; and the establishment of advanced methods for monitoring and reporting on key risks.

All of the activities associated with the two approaches described above are contained in *FSA's ERM Project Plan* which discusses the three phases of ED FSA's implementation strategy, which is described below.

#### ***Phase I: Creation of ERM organization and development of ERM program***

The first phase of implementing the ERM Program at Federal Student Aid involved developing the appropriate infrastructure necessary to support a successful

enterprise risk management strategy. Key activities in this phase included:

- Obtaining sponsorship from executive management (Chief operating officer support and creation of ERM Committee)
- Establishing an ERM organization (development and approval of proposed organizational structure, creation and finalization of position descriptions, hiring activities; and acquisition of resources necessary to support this effort)
- Developing an ERM strategy to execute this program (establishing a high-level implementation plan, defining ERM vision and mission, creating project plan and key documents associated with ERM program)

#### ***Phase II: Initiation of ERM strategy and key risk activities***

The second phase of implementing the ERM program at Federal Student Aid involved the initiation of ERM strategy and key activities. Key activities in this phase include:

- Formalizing and approving strategic plan, project plan, risk categories, risk ratings (rankings), and a common risk vocabulary
- Performing high-level risk assessment
- Conducting detailed business unit risk activities based COSO ERM-Integrated Framework to identify, assess and categorize risks

#### ***Phase III: Completion of ERM framework implementation and other activities for assessing, responding to, monitoring, and reporting on risk***

The third phase of the ERM program includes the establishment of advanced risk methodologies and other strategies for assessing, responding to, monitoring, and reporting on risk across the organization. This phase involves completing all remaining activities associated with implementing the COSO-based ERM framework; using risk data to develop enterprise-level reports for senior management; and utilizing advanced techniques, financial models, or other innovative methods to assess, monitor and manage risks. It also involves completing initial risk activities as well as developing methodology, planning for, and conducting the additional COSO activities including: risk response, control activities, communication, and monitoring. At the conclusion of these efforts, Federal Student Aid's ERM framework will be complete. This

should enable the organization to realize many of the benefits associated with an effective ERM program and will result in the development of key risk reports that provide management with an integrated or portfolio view of risk across the organization.

## **Insights from the FSA Experience**

To get started with ERM, agencies should be patient and not be discouraged if the initiative starts out slowly. ERM is not a short-term project and will require a cultural change. “Two key things to keep in mind are to expect resistance and not to oversell ERM benefits,” says Dore. “ERM is a dynamic process that continues to evolve. The real value is realized when it becomes a regular part of everyday business,” he adds.

Federal Student Aid is continually reviewing oversight and monitoring procedures for Title IV programs to ensure adequate safeguards are in place to protect program resources. Creating an enterprise risk management function has provided greater organizational strategic risk identification and assessment capabilities in their goal of working with the higher education community to lower the incidence of default in Title IV loan programs.

# Findings and Recommendations

While the basic concepts of ERM may seem straightforward, the techniques can be challenging to implement. In an examination of the financial risk management structures for Ginnie Mae and the USDA Risk Management Agency, Buttimer (2001) wrote, “an organization that contemplates instituting a ... risk management system will have a wide range of techniques and tools at its disposal, and frequently there is the temptation to immediately begin implementing those tools and techniques. Unless the organization faces the most trivial ... risks ... it is usually a mistake to rush straight into implementation.”

For ERM to work there must be a full understanding of the organization’s risk profile, its culture, and its resource capacity to implement and sustain such an initiative. It would also require that the silo and stovepipe approach to risk assessment be replaced with an open dialogue and collaborative effort that engages stakeholders when identifying and managing risks at the enterprise level.

## Findings

**Finding One: Educating a workforce unfamiliar with the ERM terminology and concepts is a key issue for leading ERM activities.** ERM is the discipline used to reduce uncertainty, which statistically and materially shifts the odds of success over time to organizations with demonstrated risk management competency. As organizations’ competency levels improve, so do the odds of successfully managing the entire spectrum of risks (RIMS, 2008).

Across the board, ERM leaders at the Centers for Disease Control (CDC) and Department of Education (ED) cited education and training as critical components of the ERM model. Both agencies have launched some formal or informal training initiative

to address this need. Various techniques used include providing presentations to Executive Committees and other specialized groups; instituting open enrollment courses that integrate ERM with internal control frameworks, and designing competency-based ERM courses tailored to specific job series.

Initially, stakeholders will have a higher learning curve than that of the typical risk expert found in organizations such as Ginnie Mae. This is not uncommon. An effective training and education plan will help equip these stakeholders with the knowledge and information needed to not only apply risk management to their day-to-day jobs, but to help champion the ERM effort across the organization horizontally and vertically. Thus, it is essential that key stakeholders (managers, supervisors, employees) understand the scope, purpose and benefits of ERM as well as the challenges and opportunities.

**Finding Two: Most ERM initiatives were not championed specifically by the chief financial officer (CFO), though the CFO was part of the ERM governance structures.** This is expected to change as the leadership role of the CFO in federal agencies is expected to expand collaboratively across organizations. According to the AGA Annual CFO Survey (2009) conducted by the Association of Government Accountants (AGA) and Grant Thornton, the future CFO can expect to collaborate more with external stakeholders such as other government entities, oversight groups and legislative bodies. Furthermore, CFOs will be expected to employ a risk management approach, for both the long and the short term and make risk analysis a first order of business.

In agencies where ERM efforts may be championed by the CFO, successful implementation will require



additional collaborations beyond the auditing and financial community. Agencies should be prepared to include and forge partnerships with these additional communities and project ERM as a strategic management tool and not as an internal auditing exercise.

**Finding Three: How organizations approach ERM may largely depend on the agency’s management objectives, resources, culture and risk tolerance level as well internal and external influences.**

A few common ERM drivers across the federal government include OMB Circular A-123, the

President’s Management Agenda, Improper Payments Act, Data Security/ID Theft, and external threats. Taking this into consideration and depending on their motivations, ERM efforts will vary in scope and scale from agency to agency.

For instance, while some agencies are mandated to focus on financial risk management (i.e., the USDA Risk Management Agency), others may opt to tailor their ERM efforts to major programs with critical financial implications, such as the Department of Education’s Federal Student Aid.

### ERM Best Practices in Federal Agencies

#### Getting Started

- Develop a risk management lexicon to ensure consistency of terminology across the organization
- Establish a communications plan and stick with it
- Don’t underestimate the level of effort or short change the planning process
- Customize ERM strategy, approach and methodology based on the specific requirements of your organization
- Support from senior leadership is critical to effectively identifying and addressing risks and opportunities
- Train your employees

#### Organizing for ERM

- Establish a Risk Office or ERM organization
- Have a dedicated “risk champion” with good communication skills
- Head of the risk organization / “risk champion” should be a member of executive management
- Establish and maintain executive level support, ideally from the highest levels in the organization

#### Operating an ERM Program

- Develop a policy that outlines the organization’s expectations regarding the management of risks
- Document the process and analysis so that it can be replicated
- Provide specific examples of risks tailored to the organization to help the learning process
- Reward risk identification, don’t penalize it: This is critical to changing the culture to effectively establish an agency-wide ERM process
- Engage those who manage risks, as well as areas with inherent risks, to develop analytical tools and recommendations: These stakeholders often know the consequences of effective and ineffective risk management, and have the rigor in thinking and planning to address risks
- Link risk training to business results where possible
- Seek diverse perspectives on issues, as they are critical to risk and opportunity management

For many agencies, it will take a holistic approach across the entire organization to realize the full impact of risk management. For others, having some variation of ERM, no matter the scale or scope, will be enough to point the agency in the right direction towards better performance, management, and results. In either case, all agencies aim to redefine how their organizations do business and will act as change leaders for the challenges that lie ahead of 21st century government.

Likewise, the effort at the IRS is centered on the integration of ERM as tool to support the agency's strategic planning, budgeting, and decision-making process, while the Centers for Disease Control and Prevention (CDC) aims to institute a model that builds and sustains public trust in the agency. Regardless of the focus, each agency shares a common goal: To establish an ERM model that provides a standardized and integrated process for identifying, mitigating and managing a portfolio of the highest risks for and within their organizations. It is certain that as agencies continue to mature their

ERM models, these ERM approaches and objectives may expand and change over time.

## Recommendations

Managing risk is imperative for successful leadership. Leaders must develop processes like ERM to improve their ability to manage risks effectively. ERM cuts across an organization's silos to identify and manage a spectrum of risks.

Risk management is not a new phenomenon within the federal sector. Many agencies have engaged in

## Implementing the Process

Agencies should consider the following relevant action steps for jumpstarting the process (adapted with changes from Walker and Shenkir, 2008):

1. **Resolve to proactively manage risks rather than to react to them.** Implementing ERM takes total commitment by management, as well as recognition by the board of its responsibility.
2. **Clarify the organization's risk philosophy.** Organizations need to know their risk capacity in terms of people capability and capital. The board and management must come to an understanding, factoring in the risk appetite of all significant stakeholders.
3. **Develop a strategy.** Since risk relates to events or actions that jeopardize achieving the organization's objectives, effective risk management depends on an understanding of the organization's strategy and goals. One of the benefits of ERM implementation is the revelation that those responsible for achieving the objectives have varying degrees of understanding about them. ERM helps get everyone on the same page.
4. **Think broadly and examine carefully events that may affect the organization's objectives.** This involves taking your business and industry apart. Pore over your strategy, its key components and related objectives. Use a variety of identification techniques such as brainstorming, interviews, self-assessment, facilitated workshops, questionnaires and scenario analysis. Start with a top-down approach. Begin to identify risks through workshops or interviews with executive management and by focusing on strategies and related business objectives.
5. **Assess risks.** Initially try to reach a consensus on the impact and likelihood of each risk. Placing risks on a risk map can be a valuable focal point for further discussion. As the risk assessment process matures, consider applying more sophisticated risk measurement tools and techniques.
6. **Develop action plans and assign responsibilities.** Every risk must have an owner somewhere in the organization. Manage the biggest risks first and gain some early wins.
7. **Maintain the flexibility to respond to new or unanticipated risks.** Put a business continuity and crisis management plan into place. If your organization is in a volatile environment, you should anticipate even more unknowns.
8. **Use metrics to monitor the effectiveness of the risk management process where possible.**
9. **Communicate the risks identified as critical.** Circulate risk information throughout the organization. The board of directors, senior assessment team and audit committee should be given regular reports on the key risks facing the organization. It is not acceptable to identify important risks and never communicate them to the appropriate people.
10. **Embed ERM into the culture.** Integrate the knowledge of risks in your internal audit planning, balanced scorecards, budgets and performance management system. Leverage your agency's compliance with OMB Circular A-123 to benefit ERM implementation.

the business of risk management for some time. What is new is the integration of risk management systems throughout the entire organization, coupled with cross-collaborations regarding risk impact from all functions within an organization. This is known as ERM.

As the external environment and challenges continue to grow, so will the expectations of stakeholders. This will require a government structure that responds quickly to changing events, is transparent and accountable. It will also require agency leadership to take a long-term view regarding their strategic objectives and the threats and opportunities that await them. The recent failures of the financial markets are an indication that effective risk management is not dependent upon a workforce responsible for carrying out risk-oriented tasks, but must be recognized and mitigated within an organization's processes and systems as well. ERM has been recognized as the bridge to make this connection.

The effort to integrate risk management throughout the organization and tying risk processes together through ERM will separate adaptable and responsive organizations from stagnate ones. Many agencies have succeeded in meeting compliance requirements through the completion of risk assessments within individual silos, or at assessing a specific risk area that crosses multiple functions (i.e. IT across an agency), but few have accomplished the integration of a risk management system throughout the organization; vertically and horizontally, including the white spaces. The agencies profiled in this study have time to reach that level of maturity and are off to a good start in recognizing the significance of ERM, the benefits, and the lessons learned if not executed correctly. Nevertheless, as ERM continues to evolve in the federal sector, agencies and their various stakeholders will benefit as a whole over time.

Based on the findings in this study, the following recommendations are offered:

1. **Establish a short and long term strategic plan for ERM.** ERM effectiveness is a matter of maturity. It takes time. Make sure stakeholders understand that ERM is a process that is strengthened over time.
2. **When considering ERM, agencies must establish a tone at the top within the organization.** Without senior leadership support, it will be difficult to get buy-in throughout the organization. Thus, ERM will be seen as another task and paper exercise rather than a strategic management process.
3. **When adopting ERM, make sure the benefits are communicated to stakeholders.** Besides compliance, demonstrate how ERM can enhance organizational performance, heighten awareness about risk management, improve workforce skill sets, and create a "safe place" for managers to discuss risk management outside of their comfort zones.
4. **Collaborate within and across other agencies.** Don't work in a vacuum. Find agencies with similar operational functions or missions and benchmark risk management practices. Join organizations that advocate ERM and provide resources for continuous learning in this subject matter (e.g., FederalERM.com).
5. **Don't reinvent the wheel.** Use what you have. If there is an existing internal control framework in place, build upon that. Strategize about how ERM can enhance or strengthen your existing internal control environment.
6. **Have experienced staff available to champion and carryout the vision of the ERM process.** A knowledgeable workforce is the key to successful ERM implementation. If you cannot hire new staff, retrain the staff that you have.
7. **Communicate short wins immediately.** Nothing reinforces success like results. Show stakeholders how ERM has led to successful identification and mitigation of risks, business opportunities or cost savings.

# Appendix: Survey of Risk Management Skills

## Risk Manager Core Competency Survey

A survey of ERM leaders at select agencies was conducted to help scan the environmental conditions under which ERM adoption was being implemented. The *Federal Risk Manager Core Competency Survey* was designed to collect feedback from the leaders involved in the ERM process. The survey design was based on the Risk and Insurance Management Society's (RIMS) Risk Manager Core Competency Model and was modified to reflect the dynamics and operations of federal agencies. The RIMS model reflects components of the best practices and best theoretical models, preferred by the RIMS Fellow Advisory Council, the American Society for Training and Development, and basic business management texts. The RIMS model takes the best ideas from many models and modifies them to reflect the many different skills required for risk management.

The *Federal Risk Manager Core Competency Survey* consisted of two sections: (1) Demographics, and (2) an Assessment of Conceptual, Core Competency, and Technical Skills for Risk Managers.

## Conceptual, Core Competency and Technical Skills

With exception to Conceptual and Technical Skills, the group of Core competency skills is broken into three sub-categories:

- Interpersonal skills
- Personal skills
- Business skills

A description of each skill set is presented in Figure A-1.

The *Federal Risk Manager Core Competency Survey* was based on a modification of the RIMS model to reflect the dynamics of the federal workforce, therefore not all skills are included in the survey responses.

## Survey Findings

### Finding One: Leadership Experience and Resources.

ERM agency leaders are generally supervisors with 2-5 years experience in their current positions. Most have from 2 to 10 years experience in the area of risk management, internal controls, auditing or financial management. Their role in the ERM process includes being a sponsor within the agency to advocate for a standard ERM process and leading cross-cutting, high level strategic workgroups to develop the process. Most of the work involved with the ERM initiative is executed by 2-5 staff members who are full- and part-time. No contract support has been acquired to facilitate the ERM effort. There is no specific budget set aside for ERM.

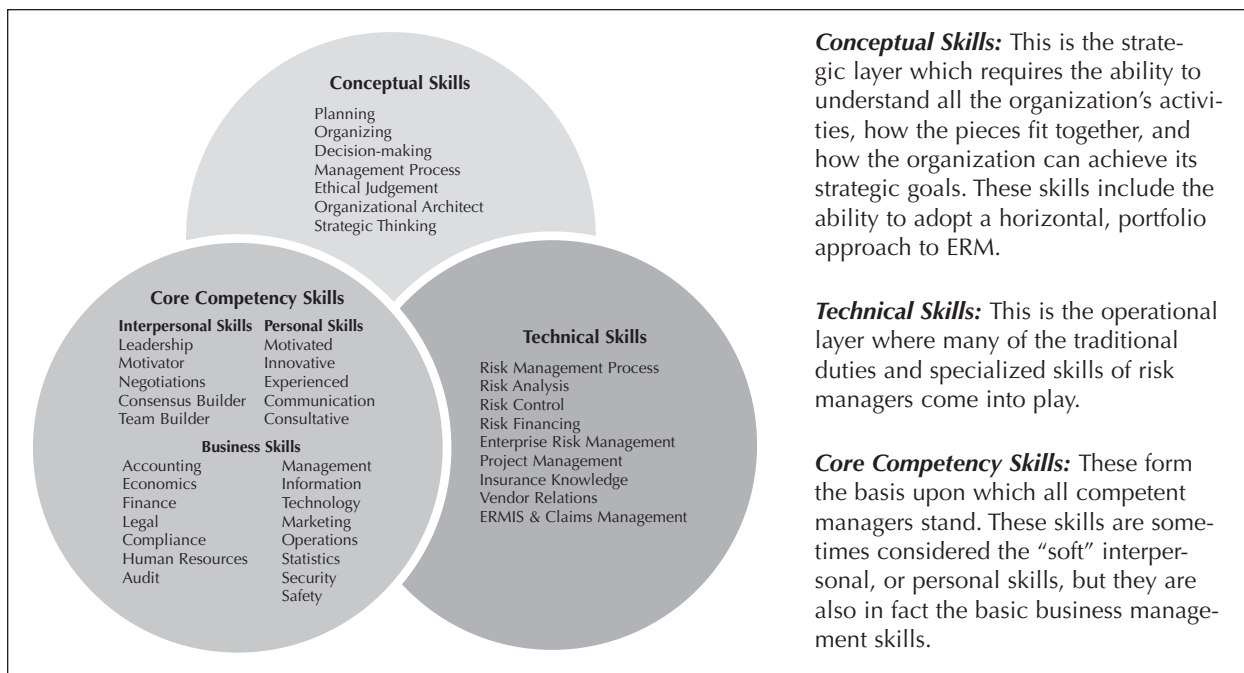
### Finding Two: ERM Scope and Standardization.

ERM efforts within agencies either span across a single program and/or administrative area or cuts across the entire agency. No leader identified the effort as spanning across multiple programs and/or administrative areas. ERM leaders identified the COSO Enterprise Risk Management Framework as the application technique for adopting ERM within their agencies.

### Finding Three: Subject-Matter Awareness.

ERM leaders identified an awareness of the following resources as beneficial to their leadership effectiveness: Sarbanes-Oxley, OMB Circular A-123, FMFIA (Federal Manager's Financial Integrity Act), Chief Financial Officer (CFO) Act, GAO Internal Control

**Figure A-1: Risk Manager Core Competency Model**



Source: RIMS.org. Reprinted with permission.

Management and Evaluation Tool, and the GAO Standards for Internal Controls.

**Finding Four: ERM Opportunities and Challenges.**

Agency ERM leaders identified the adoption of risk management, improved operations, and a cultural understanding of the importance of sustaining high credibility as opportunities of ERM. Challenges included convincing managers that risk management is a good idea, insufficient sponsoring at the executive level, the perception of adding the burden of another task, and providing the appropriate ERM foundation, assessment and management platform.

**Finding Five: Strategic Planning.**

While no long-term strategic planning is yet in the works for agencies in the early stages of ERM, leaders identified several strategic tools being used to aid, integrate and introduce ERM within their organizations. Specific tools include having a Change Management Plan, Communications Plan, Training and Education Plan, and inter-agency collaborative workgroups.

**Finding Six: Skill Assessment.**

With exception to *economics and statistics*, agency ERM leaders would recommend most of the skills identified in the competency model. Feedback regarding Technical Skills suggest that most ERM leaders would benefit

from additional knowledge and training in areas specific to risk management, such as *risk analysis, risk financing, risk management information systems, and project risk management*. For Conceptual Skills, respondents identified *planning* and *organizing* as areas for additional knowledge. Key business skills that a few agency leaders were not applying but would recommend include *accounting, budget and finance, strategic planning and auditing*.

# Endnotes

1. For more in-depth descriptions of the GAO Risk Management Framework, visit <http://www.gao.gov/new.items/d0691.pdf>
2. For a copy of the ISO 31000 Standard, visit <http://www.iso.org>.
3. To gain more in depth information and details about the three dimensions and application techniques, visit <http://www.aicpa.org>.

# References

- Association of Government Accountants (AGA). Annual CFO Survey. Financial Management: Providing a Foundation for Transition. July 2008.
- Association of Government Accountants (AGA). Annual CFO Survey. Recovery and the Transparency Imperative. July 2009.
- Beasley, Mark S., Bruce C. Branson, Bonnie V. Hancock. 2008. Rising Expectations: Audit committee oversight of enterprise risk management. *Journal of Accountancy*: 46-47. April 2008.
- Beasley, Mark, Bruce Branson, Bonnie Hancock. 2009. *Report on the Current State of Enterprise Risk Oversight*. ERM Initiative at North Carolina State University.
- Buttimer, Richard J. 2001. *Financial Risk Management in the Federal Government: Overview, Practice, and Recommendations*. IBM Center for the Business of Government.
- Charette, Robert. 2009. On the Look Out: If government's job is to protect the people, it must begin to manage risk-before disaster strikes. In *Government Executive Magazine*: 28-34. March 2009.
- CDC mission statement. Available at <http://www.cdc.gov/about/organization/mission.htm>
- CDC organizational chart. Available at <http://www.cdc.gov/about/leadership/leaders/garland.htm>
- COSO. 2004. Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management- Integrated Framework: Executive Summary*. Available at <http://www.aicpa.org>.
- Department of Education mission statement. Available at <http://www.ED.gov/about>.
- Department of Education. 2006. Federal Student Aid Five-Year Plan (2006-2010). Available at [http://www.ed.gov/about/offices/list/om/fs\\_po/fsa/intro.html#2](http://www.ed.gov/about/offices/list/om/fs_po/fsa/intro.html#2)
- Department of Education. 2007. Agency Strategic Plan. Available at <http://www.ed.gov>.
- Department of Housing and Urban Development (HUD). Press Release # HUD 09-177: September 18, 2009. <http://www.hud.gov/news/index.cfm>
- DHHS. 2008. Guidance Manual for OMB Circular A-123 Assessments. January 2008.
- Dore, Stan., Cynthia Vitters. U.S. Department of Education's Federal Student Aid. Interview with Karen Hardy. March 20, 2009.
- Dore, Stan. 2006. Enterprise Risk Management: What's All the Buzz About? Department of Education Federal Student Aid Presentation given at the 2006 AGA Internal Control & Fraud Conference.
- Eccles, Robert G., Scott C. Newquist, Roland Schatz. 2009. Reputation and Its Risks. *Harvard Business Review OnPoint*: 97-108. Spring 2009.
- Federal Risk Manager Core Competency Survey. 2009.
- Fox, Christopher. 2009. A Guide to Starting an ERM Program. Available at <http://www.rmmag.org>. May 14, 2009.

- GAO. 2001. *Performance and Accountability Series: Major Management Challenges and Program Risks for the Department of Education*. January 2001. GAO-01-245.
- GAO. 2005. *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*. GAO-06-91.
- GAO. 2009. *Privacy and Security: Food and Drug Administration Faces Challenges in Establishing Protections for Its Postmarket Risk Analysis System*. GAO-09-355.
- Garland, Donna G. Centers for Disease Control and Prevention. Interview with Karen Hardy. December 29, 2008.
- Garland, Donna G. 2008. *Risk Recognition and Mitigation: Making CDC RiskSmart*. Office of Executive Communication's PowerPoint presentation to the CDC leadership.
- Ginnie Mae mission statement. Available at <http://www.ginniemae.gov/about/about.asp?Section=About>
- Gjerdrum, D. "An Overview of ISO 31000:2009-International Standard on the Practice of Risk Management." In press, *PRMIA Magazine*.
- Hess, Christopher J. 2007. OPERA PowerPoint presentation at North Carolina State University's ERM Roundtable. May 21, 2007.
- Hess, Christopher J. 2009. Internal Revenue Service. Interview with Karen Hardy. May 5, 2009.
- IRS. 2000. *Modernizing America's Tax Agency: IRS Organization Blueprint 2000*. Available at <http://www.irs.gov/pub/irs-utl/27877d00.pdf>
- National Transportation Safety Board (NTSB) mission statement. Available from [NTSB.gov](http://NTSB.gov).
- OMB. 2004. *Revisions to OMB Circular A-123, Management's Responsibility for Internal Control*. December 21, 2004.
- Peter, Mary, Dorothy Gjerdrum, Katharine Peeling. 2009. Eeny, Meeny, Miny, Moe – Catch a Standard by the Toe. Presentation at the RIMS 2009 Conference. April 22, 2009.
- Pickett, Spencer K.H. 2006. *Enterprise Risk Management: A Manager's Journey*. Hoboken, NJ: John Wiley & Sons.
- RIMS Risk Manager Core Competency Model. 2007. Available at <http://www.rims.org/education>
- RIMS, 2009. *The 2008 Financial Crisis: A Wake-up Call for Enterprise Risk Management*. Executive Report. Available at <http://www.rims.org>.
- RIMS, 2008b. Press Release. *Groundbreaking Study Validates Enterprise Risk Management Boost To Business Performance*. New York. November 20, 2008. PR Newswire.
- Risk and Insurance Management Society (RIMS). 2008 State of ERM Report—Executive Summary. Available at <http://www.RIMS.org>.
- Solomon, David. (2008). Perspectives on the current environment and risk management. The Conference Board 2008 Enterprise Risk Management Conference.
- Treasury Board of Canada Secretariat. 2001. *Integrated Risk Management Framework*.
- USPS mission statement. Available at <http://www.usps.gov>.
- Walker, Paul L., William G. Shenkir. 2008. Checklist: Implementing Enterprise Risk Management. *Journal of Accountancy*: 31. March 2008.



# Acknowledgements

The author would like to express gratitude to the IBM Center for The Business of Government for supporting this work. Many people contributed valuable time, comments, feedback and background information to ensure successful completion of this report; specifically Donna Garland, Stan Dore, Cynthia Vitters, Christopher Hess, Patricia McGuire, Sallyanne Harper, Michael Trouper, and Mark Abramson and the IBM Center staff.

## ABOUT THE AUTHOR

**Dr. Karen Hardy** is a Visiting Scholar at Strayer University. She has over 20 years of experience in the public sector and spent several years in the private sector in the area of commercial banking. Hardy is the author of a multitude of publications including the book *Building Self-Leaders*, which takes a look at the management succession process in the federal government and provides a model training program for addressing leadership issues.

Hardy is a scholar-practitioner and social scientist focusing on research in the areas of leadership and business. She has collaborated with researchers at Virginia Tech University in expanding self-leadership theory and practice.

Her research has been cited and published in the *Journal of Managerial Psychology* and featured in *Government Executive Magazine*. She has written articles for *The Public Manager* and *FedTech Magazine*. Hardy is a member of the Federal Executive Steering Group for Enterprise Risk Management and of the FederalERM.com community. She is also a member of the Academy of Human Resource Development and the Phi Gamma Sigma Professional Society.

Hardy earned her doctorate in Organizational Leadership and Human Resource Development from Nova Southeastern University and her Masters in Business Administration from Strayer University.



## KEY CONTACT INFORMATION

### To contact the author:

**Dr. Karen Hardy**

Visiting Scholar, Strayer University  
10721 Elizabeth Parnum Place  
Upper Marlboro, MD 20772  
240-462-3383

e-mail: [drkarenhardy@yahoo.com](mailto:drkarenhardy@yahoo.com)

website: [drkarenspeaks.com](http://drkarenspeaks.com)



For a full listing of IBM Center publications,  
visit the Center's website at [www.businessofgovernment.org](http://www.businessofgovernment.org).

Recent reports available on the website include:

### **Analytics**

*Strategic Use of Analytics in Government* by Thomas H. Davenport

### **Collaboration: Networks and Partnerships**

*Designing and Managing Cross-Sector Collaboration: A Case Study in Reducing Traffic Congestions* by John M. Bryson, Barbara C. Crosby, Melissa M. Stone, and Emily O. Saunoi-Sandgren

*Integrating Service Delivery Across Levels of Government: Case Studies of Canada and Other Countries* by Jeffrey Roy and John Langford

### **Contracting**

*The Challenge of Contracting for Large Complex Projects* by Trevor L. Brown, Matthew Potoski, and David M. Van Slyke

### **Defense**

*Transformation of the Department of Defense's Business Systems* by Jacques S. Gansler and William Lucyshyn

### **E-Government/Technology**

*Moving to the Cloud: An Introduction to Cloud Computing in Government* by David C. Wyld

### **Financial Management**

*Managing a \$700 Billion Bailout: Lessons from the Home Owners' Loan Corporation and the Resolution Trust Corporation* by Mark K. Cassell and Susan M. Hoffmann

*Strengthening Government's Ability to Deal with the Financial Crisis* by Thomas H. Stanton

### **Healthcare**

*The Role and Use of Wireless Technology in the Management and Monitoring of Chronic Diseases* by Elie Geisler and Nilmini Wickramasinghe  
*Creating Telemedicine-Based Medical Networks for Rural and Frontier Areas* by Leonard R. Graziplene

### **Human Capital Management**

*Federated Human Resource Management in the Federal Government* by James R. Thompson and Rob Seidner

### **Managing for Performance and Results**

*Performance Reporting: Insights from International Practice* by Richard Boyle

*Strategic Risk Management in Government: A Look at Homeland Security* by David H. Schanzer, Joe Eyerman and Veronique de Rugy

### **Organizational Transformation**

*Launching a New Mission: Michael Griffin and NASA's Return to the Moon* by W. Henry Lambright

### **Social Services**

*US and UK Routes to Employment: Strategies to Improve Integrated Service Delivery to People with Disabilities* by Heike Boeltzig, Doria Pilling, Jaimie C. Timmons, and Robyn Johnson

### **About the IBM Center for The Business of Government**

The IBM Center for The Business of Government connects public management research with practice. Since 1998, we have helped public sector executives improve the effectiveness of government with practical ideas and original thinking. We sponsor independent research by top minds in academe and the nonprofit sector, and we create opportunities for dialogue on a broad range of public management topics.

The Center is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Center focuses on the future of the operation and management of the public sector.

### **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 business value. For more information visit [www.ibm.com](http://www.ibm.com).

### **For additional information, contact:**

#### **Jonathan D. Breul**

Executive Director

IBM Center for The Business of Government

1301 K Street, NW

Fourth Floor, West Tower

Washington, DC 20005

(202) 515-4504, fax: (202) 515-4375

e-mail: [businessofgovernment@us.ibm.com](mailto:businessofgovernment@us.ibm.com)

website: [www.businessofgovernment.org](http://www.businessofgovernment.org)