Federal Risk Management: Under Construction

By John M. Kamensky

"By some estimates, taking out just nine critical electrical substations could plunge the whole nation into darkness," says Jason Black, a researcher at Battelle Institute. This scenario, of course, probably keeps the leaders of the Federal Energy Regulatory Commission (FERC) awake at night. What is their risk management strategy?

Other federal agencies also face a wide range of risks. Some are external; others are internal to an agency:

- Some risks are financial (such as having to deal with managing under a federal sequester or the financial market's impact on corporate investments in pension funds, which could affect federal pension guarantees).
- Some are operational, such as those faced by FERC, or cybersecurity threats, or even insider threats by employees.
- Some are reputational, such as the recent accusations of Patent Office telework abuse, or the General Services Administration's lavish conferences scandal.

In recent years, a number of federal agencies have put risk management strategies in place. In fact, recent guidance from the Office of Management and Budget (OMB) declares that "Agencies are expected to manage risks and challenges related to delivering the organization's mission." However, individual federal agencies haven't been waiting for governmentwide policies to be put into place. They are doing it on their own, in their own context. Some—like the Department of Commerce—have created central offices to develop risk management policies. Others—like the Office of Federal Student Aid in the Department of Education—have designated a chief risk officer and created a risk management council of top agency officials that meets regularly. In addition, a professional association has evolved—the Association for Federal Enterprise Risk Management—through which federal managers from across the government can share insights and trade best practices.

While there is no overarching federal policy on risk management, David Mader, OMB's top finance officer, says that, in early 2015, OMB will offer more specific guidance to agencies regarding risk management. With guidelines "under construction," what are some of the issues in play?

Risk is a Fact of Life

Risk is inherent in every facet of society. In our personal lives, there are risks to health from eating bad foods, risk of injury or damage from driving a car or living in a zone where extreme weather events (hurricanes, tornadoes, floods) occur, and, in the modern world, risk of financial or identity theft or other types of financial theft due to online banking fraud. People understand that such risks are inherent and generally support action to reduce the impact of those risks, such as standards for food inspections, building safer cars and

John M. Kamensky is Senior Fellow at the IBM Center for The Business of Government.

homes, and paying fees to banks to help defray the cost of online fraud.

Successful commercial enterprises assess the risks they face, and develop responses to manage those risks. These range from paying insurance in advance so that they can recover losses, to moving to less risky methods of production (which can reduce costs associated with an unsafe workplace). Other responses to informing the public in advance that a risk may occur and what will happen if it does (such as when credit card companies tell individuals in advance about loss limits if their online accounts are compromised).

In the government, risks have been primarily seen as constraints to minimize, avoid, or hide in a corner. With the exception of agencies such as the Federal Emergency Management Agency (FEMA), whose mission is to respond to risks when they occur, most federal agencies tend to attempt risk *reduction* rather than risk *management*. As a result, when something goes wrong—which, given the world in which we live, will inevitably occur—agencies, their constituents, and their overseers often react to the immediate problem, rather than understanding in advance how to develop strategies to respond to issues that will arise.

What is "Enterprise Risk Management?"

Risk management is an evolving area in government. It involves the creation of a new common language, and the reconciliation of different definitions of success among different professional disciplines within government. Going forward, the key to success will be developing a shared understanding of risk management.

Risk management expert Doug Webster writes, "... Many of us think of risk only in terms of bad consequences", but "the word has evolved to refer to two different and conflicting concepts." He observes that the U.S. Government Accountability Office's definition "treats risk as introducing only a negative impact .... Risk management in this context is typically focused on managing threats to the achievement of objectives managing the threats to objectives." However, he continues, "Risk management professionals are more likely to subscribe to the definition offered by the international standard ISO 31000, which defines risk as 'the effect of uncertainty on objectives."

John Fraser, senior vice president of a Canadian hydro-electric company, Hydro One Networks, says that effective enterprise risk management can be distilled down to two essential processes: having conversations and setting priorities. He says, "By enlisting managers and employees in conversations, organizational leaders can facilitate people's willingness and ability to [bring to the] surface major risks so that they can be addressed. Then, by prioritizing these known risks the organization can allocate its energy to addressing the most important risks ... in a systematic way."

Different Approaches to Risk Management

There seem to be three different approaches to developing a risk management strategy:

Setting Standards and Policies. Some governments, such as the United Kingdom and Australia, have focused on the development of definitions and principles. Other organizations have adopted commercial standards, such as ISO 31000. While this has not been the approach in the U.S. government, the financial community has developed internal control standards.

Defining Roles and Creating a Governance Framework. In countries such as Australia, there is a focus on creating a governance structure that engages top leadership on a regular basis in discussions about potential near-term and long-term risks. These provide forums for the use of analytics and real-time data. This approach has been adopted by the U.S. Department of Education's Office of Federal Student Aid, which pioneered the use of a chief risk officer. There, the role of a chief risk officer is to advise agency leadership on the potential impact of risks across the office's portfolio of programs; this is not the traditional approach of examining risks within each individual program or function.

Using Multiple Disciplinary Approaches. Another element in designing a risk management approach is ensuring the "voices" of different professional disciplines within an organization are heard. This might include staff with strategic foresight and planning backgrounds, those with performance, analytical, and evaluation backgrounds, and those with mission delivery responsibilities.

Risk Frameworks: The British Example

In 2002, British Prime Minister Tony Blair launched a two-year "risk program" to develop a set of principles and concepts, culminating in the risk management "Orange Book" in 2004. Several years later, this was supplemented with an in-depth guide book. This program serves as an overarching framework for developing risk management strategies for British government agencies.

For example, one British agency, National Savings and Investments, identified 13 key risks and assigned responsibility for each to an executive director. Every six months, the board conducts a review. Individual projects have their own "risk registers" as well as joint project teams. This allowed the agency to keep abreast of changes in the external environment and develop contingency plans for various scenarios.

Australia's Nine Risk Management Elements

More recently, the national government of Australia issued a policy document in July 2014, which outlines a set of principles that each government agency must incorporate into how it runs its programs (the government also provides accompanying resources to help its agencies develop effective programs).

The Australian government's goal is to "embed risk management as part of the culture of Commonwealth entities where

The Risk Management Policy for the Commonwealth of Australia

Establishing a risk management policy that defines an entity's approach to risk and explains how this supports its strategic plan.

Establishing a risk management framework that provides the foundations and organizational arrangements for designing, implementing, monitoring, and continually improving.

Defining responsibility for managing risk by defining roles and responsibilities for individual implementation tasks.

Embedding systematic risk management into business processes, including but not limited to strategic planning, policy development, program delivery, and decision making.

Developing a positive risk culture that promotes an open and proactive approach to considering both threat and opportunity.

Communicating and consulting about risk with relevant stakeholders and transparent, complete, and timely flows of information between decision makers.

Understanding and managing shared risks that extends beyond a single entity and requires shared oversight and management.

Maintaining risk management capability to preserve an appropriate level of capacity to manage an entity's risks, commensurate with its risk profile.

Reviewing and continuously improving the management of risk so that it is not seen as a "one- off event" but as a process of continuous improvement, based on internal reviews.

the shared understanding of risk leads to well informed decision making." To do this, it set forth nine elements with which all agencies must comply (see accompanying text box).

The Risk of Risk Management

There is the danger of a risk management initiative becoming a cumbersome, formulaic, and unhelpful exercise. "Over-dependence on process may limit departments' ability to manage risk effectively," notes the UK National Audit Office. "... Effective risk management offers a means of anticipating issues and responding to them."

Webster notes that the biggest danger in introducing an enterprise risk management requirement is creating a function that is seen as a compliance hoop, rather than a culture change. To be effective, it has to be leader-driven. But, having an individual leader to serve as its champion does not span leadership transitions very well—which is the strength of establishing standards and requirements. Nevertheless, creating standards and policies introduces the danger of enterprise risk management becoming a compliance-oriented administrative function.

Potential Next Steps

Should the U.S. government undertake its own effort to create a governmentwide risk-responsive framework? At a recent forum, Tom Stanton, co-author of a new book on risk and performance in government, observed that this may not be a good idea. He feels that mandating a governmentwide framework—such as requiring the use of the ISO standards—poses the risk of creating a compliance-oriented system, not a change in how agency leaders manage. His advice is to develop risk management frameworks at the bureau level, within the context of each bureau's mission and environment.

However, developing a governmentwide set of risk principles—much like Australia has done—might be a useful approach for the federal government. Todd Grams, a well-respected former federal executive, recently observed, "It's difficult for a senior management team to manage risk if they don't have a shared understanding of what risk means." When Australia developed its policy, it engaged a broad segment of its senior executive community. It did not rely on just one professional community to outline the policy but included experienced executives with backgrounds in strategic foresight, planning, performance management and mission delivery.

As noted earlier, federal agencies aren't waiting for governmentwide policies to be put into place. They are doing it on their own, in their own context. As Stanton notes, this more organic evolution of risk-responsive frameworks may be a more appropriate approach for ensuring that these "home-grown" policies are actually used to manage risks. An overly prescriptive governmentwide approach risks becoming another compliance requirement. ◘

References

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