Trend Two: Risk
Managing and Communicating Risk

Today, given budget austerity and the complex challenges facing government executives, managing risk in the public sector has taken on new significance. Risks take many forms, including national security risks via cyberattacks, economic risks from natural disasters, budget and program risks, or privacy risks. However, government leaders lack an accepted culture and framework in which to properly manage, incorporate, and communicate risk. This tends to constrain creativity and innovation within government.

Understanding the spectrum of risks, developing strategies and tools to mitigate them, and developing strategies for communicating risks to appropriate target populations will be growing challenges for government executives in years to come. More importantly, assessing the inherent risks facing the public sector, and acting accordingly, is a key trend that can drive change in government and promote successful management of government programs and missions.

Assessing the inherent risks facing the public sector, and acting accordingly, is a key trend that can drive change in government and promote successful management of government programs and missions.

Accepting Risk as a Condition of Action

Risk is inherent in every facet of life—risks to health from bad food, risk of injury or damage from driving a car or living in a zone where extreme weather events occur, risk of financial or identity theft due to online banking fraud. David Schanzer notes in a 2010 IBM Center report:

> 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 risks 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 is, in a sense, a form of strategic risk management.

Human beings understand that such risks are inherent, and generally support action to reduce the impact of risks—standards for food inspections, safety standards for cars and homes, and banking fees to defray the cost of online fraud.

In the commercial sector, successful enterprises assess the risks that 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 (e.g., reducing the costs that are a consequence of an unsafe workplace), to informing the public in advance of potential risks and liabilities faced in the event of losses (e.g., credit card companies tell individuals in advance that if their online accounts are compromised, they will only lose up to a certain dollar amount, which increases trust in the use of cards online).

Risk is Inherent in Achieving Government Missions

In government, risks have been primarily seen as constraints to minimize or avoid. With the exception of agencies such as FEMA, which has a risk management mission, most federal agencies tend to focus on risk *avoidance* rather than risk *management*. As a result, when something goes wrong, agencies, their constituents, and their overseers tend to overreact to the immediate problem, rather than understanding in advance how to develop strategies that anticipate the inherent risks associated with the missions these agencies perform. Every agency faces financial management, worker skillset, and now cybersecurity risks; few think in advance about how to understand what may happen in these and other domains, how to communicate that in advance to their employees and stakeholders, and how to be resilient in the face of disruption.

Complicating the government picture further, a different kind of risk calculus faces the national security community every day. Managing risk in this arena is especially complex when the forms and patterns of security threats are changing in so many ways and at a faster pace than ever before. The capabilities required to threaten a nation, region, or even global stability are available to both rich and impoverished nation-states, as well as small networks of people who can and do operate independently of any nation-state. Long-range, stealthy, precision attacks—once the exclusive domain of America's military—are now available via cyberattack to a wide range of people and groups, well outside the bounds of nation-state controls.

Given the rapid pace of change that government faces, it is imperative that agencies turn from a culture of risk avoidance to one of risk management.

Turning from Risk Avoidance to Risk Management

Given the rapid pace of change that government faces, it is imperative that agencies turn from a culture of risk avoidance to one of risk management. A thought-provoking approach to how this change can occur appears in a *Harvard Business Review* article, "Managing Risks: A New Framework," by Robert Kaplan and Anette Mikes. Kaplan and Mikes note that "risk management is too often treated as a compliance issue that can be solved by drawing up lots of rules and making sure that all employees follow them." In addition, many organizations compartmentalize their risk management functions along business lines (credit risk, operational risk, financial risk) and this "inhibits discussion of how different risks interact." Such categorizations can miss many kinds of risks that organizations face.

Three Categories of Risk. Kaplan and Mikes developed a framework "that allows executives to tell which risks can be managed through a rules-based model and which require alternative approaches." Their research identifies three categories of risk.

- **Preventable.** "These are internal risks, arising from within the organization, that are controllable and ought to be eliminated or avoided." These include illegal, unethical, or inappropriate actions, as well as breakdowns in operational processes. In the federal government, these are typically covered by internal control schemes. The authors say these kinds of risks are "best controlled through active prevention: monitoring operational processes and guiding people's behaviors and decisions toward desired norms." This can be done via rule-based compliance approaches.
- **Strategic.** These differ from preventable risks because they are not necessarily undesirable. For example, developing a satellite-based air traffic control system may be seen as taking a strategic risk over the proven, ground-based radar-controlled air traffic control system. The authors say, "Strategy risks cannot be managed through a rules-based control model. Instead, you need a risk-management system designed

Emerging Discipline of Enterprise Risk Management (ERM)

Increasingly, agencies are looking to the emerging discipline of enterprise risk management (ERM) as a way to make sense of this complexity, and integrate risk strategies into their daily operations and longer-term mission priorities. As Karen Hardy notes in her report for the IBM Center, *Managing Risk in Government: An Introduction to Enterprise Risk Management*, ERM spans all aspects of an organization's activities and is:

- A process, ongoing and flowing through an entity
- Affected 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

to reduce the probability that the assumed risks actually materialize and to improve the company's ability to manage or contain the risk events should they occur."

- **External risks.** Organizations cannot prevent external risks from happening. So managers need to forecast what these risks might be and develop ways to lessen their impact. They cannot be avoided, only managed. The model for addressing external risks is the use of "open and explicit risk discussions," the authors say. The format might be war gaming (for near-term issues) or scenario analyses (for longer-term issues).

Kaplan and Mikes observe that "each approach requires quite different structures and roles for a risk-management function." One way to implement this integrative approach is to anchor risk discussions in strategic planning functions; this function already serves as integrative in most large organizations and points to positive action rather than constraints. It is about turning the conversation from risk management that "focuses on the negative" to a risk strategy that aligns with "the 'can do' culture most leadership teams try to foster when implementing strategy." Significantly, this approach aligns with the Government Accountability Office (GAO) "Risk Management Cycle." As Figure 1 indicates, the first step is to identify strategic goals, including through public engagement; then move to a more formal process of risk assessment, consideration and selection of alternative ways to address those risks, and, finally, to execution and evaluation of the chosen alternatives to inform new strategies.

Figure 1: GAO Risk Management Cycle

Four Strategies for Responding to Risks. Another approach to risk management grows out of the long-standing risk review discipline related to financial controls. This risk management framework, described by James Bailey in his IBM Center report, *Strengthening Control and Integrity: A Checklist for Government Managers*, focuses on four different strategies for responding to risks.

- Acceptance—live with the risk and accept the consequences. Can be useful for small risks

- Elimination—stop doing the activity that creates the risk; this can be useful for low-value activities.
- Transfer—Outsource activities to entities that can better perform, such as shared services for back office activities.
- Reduction—Use controls to reduce potential impacts, as done in many traditional risk and compliance programs, as well as technology and acquisition programs, by moving to modular approaches that limit risk in each program incrementally.

Tony Bovaird and Barry Quirk, in "Reducing Public Risk and Improving Public Resilience: An Agenda for Risk Enablement Strategies," as posted on INLOGOV Blog, outline a novel approach to helping government assess and manage risks as part of their strategy. This paper introduces a new concept of "risk enablement" as a means of moving toward a positive and forward-looking agenda that focuses on risks to citizens and businesses who receive government services, rather than a traditional view of risk to internal organizations. Risk enablement can help "decision-makers in the service system to choose activities with appropriate levels of risk, rather than assuming that risk minimization is always right." Related to this is the concept of building resilience into federal programs and activities, so that as risks manifest, the agency is better equipped to address them.

Getting the Word Out About Risk

A key element of addressing risks facing federal agencies involves effective risk communication. In other words, understand what risks might affect an agency's constituents, and then proactively get the word out about those risks. FEMA, for example, already exercises this strategy, advising individuals living in hurricane zones about potential outcomes, so that the public and the agency are better prepared if and when a storm arrives. If other agencies were to identify the potential risks being faced and similarly communicate them in advance, this would bring numerous benefits:

- Agencies would seek to understand risks to their constituents more completely.
- The public would have advance word on what might occur, helping to increase preparedness in the general population.
- If the risks become realities, the acceptance and public discourse is framed as one that builds around a sound response to a problem that has been forecast, rather than focusing on the reactions to an unanticipated event, which can quickly magnify the problem.

Pursuing New Areas of Research

The emergence of "big data" and a proliferation of high-performance computing open up potential new areas of research on how best to address and manage risk. The sheer power of modern technology allows an agency to understand, predict, and respond to uncertainty with far more effectiveness and at a far lower cost. Part of the future of risk enablement can be driven by analytics that can help organizations forecast, plan for, and respond to risks.

Looking forward, several important questions merit further investigation. These cover all aspects of risk management, from assessment to enablement, and include:

- Understanding various types of risk
- Being agile in the face of unanticipated risks
- New forms of risk management products and means
- New organizational forms that link public, private, and nonprofit organizations together around risk planning and response
- Training that helps prepare government leaders to think more strategically about risk as part of strategy development and implementation

The first step is to identify strategic goals, including through public engagement; then move to a more formal process of risk assessment, consideration and selection of alternative ways to address those risks, and, finally, to execution and evaluation of the chosen alternatives to inform new strategies.

Conclusion

As government operates in a world of increasing speed and complexity, and as citizens, who both empower and are served by government, expect better, faster, and more cost-effective results, addressing risk that can interfere with normal operations becomes ever more critical. The risk frameworks and strategies highlighted here can help leaders manage and respond to risks, fostering success within and across programs. In the future, such frameworks can be made real for government through partnerships with industry, nonprofits, researchers, and citizens. Tackling risk is a trend driving change in government, but challenges remain. Government executives must choose between two distinctly different paths: gain visibility of risks in advance, communicate their impacts, and be resilient in response in a way that enables positive outcomes; or be pressed into a more and more reactive mode because risks are not well-managed.

Resources

Bailey, James. *Strengthening Control and Integrity: A Checklist for Government Managers.* IBM Center for The Business of Government. 2010.

Bovaird, Tony and Barry Quirk. "Reducing Public Risk and Improving Public Resilience: An Agenda for Risk Enablement Strategies." INLOGOV Blog—Official Blog of the Institute for Local Government Studies, University of Birmingham, http://inlogov.wordpress.com/2013/07/06/bovairdquirk/.

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

Keegan, Michael J. "Analytics and Risk Management: Tools for Making Better Decisions." *The Business of Government* magazine, Spring 2010.

Keegan, Michael J. "Analytics and Decision Making: A Conversation with Tom Davenport, Distinguished Professor in Information Technology and Management at Babson College." *The Business of Government* magazine, Spring 2010.

Kaplan, Robert and Anette Mikes. "Managing Risks: A New Framework." *Harvard Business Review*, 2012.

Schanzer, David and Joe Eyerman, *Strategic Risk Management in Government: A Look at Homeland Security*. IBM Center for The Business of Government. 2010.

A Video Overview of Analytics and Risk Management. The IBM Center for The Business of Government. 2010.