Driver Four: Risk

Mitigating risk, managing cybersecurity, and building resiliency to meet the mission of government

The safety and security of the nation faces threats from an array of hazards, including acts of terrorism, malicious activity in cyberspace, pandemics, manmade accidents, transnational crime, and natural disasters. Many federal agencies carry out missions to stay ahead of these risks and mitigate their impacts. In addition, government leaders responsible for managing complex and risky missions must also address and mitigate internal risks in a dynamic and uncertain world.

Within this context, government leaders operate in an environment of increasingly intricate and interconnected systems. Devices have become smarter and more interconnected to the external world. Government leaders must build the capability and capacity to identify, understand, and address risks and potential threats. Assessing the inherent risks facing the public sector, and acting to mitigate and respond to those risks, can promote successful management of programs and missions and facilitate the transformation of operations.

With uncertainty facing government widening and deepening, external and internal risks pose threats to achieving an organization's goals and objectives.

Increased Risks and Threats Facing Government

Risk involves the effect of uncertainty on objectives. With uncertainty facing government widening and deepening, external and internal risks pose threats to achieving an organization's goals and objectives. Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political domains, as well as a broad range of operational risks such as information security, human capital, and business continuity.

- **External Risks.** Environmental factors as diverse as an aging workforce, changing social norms, or increased cyber security threats impact federal agencies in multiple ways. These changes occurring in the external environment produce numerous risks over which the organization has little to no direct control. Having limited control over external risks, however, does not mean ignoring them. Instead, agencies should assess external risks as part of evaluating the achievability of future goals and considering alternative approaches to reaching those goals.
- **Internal Risks.** In addition to mission risks caused by events outside the organization's control, other internal risks can be affected by organizational actions. These actions include internal processes, such as controls, training, values and culture, and are under the direct influence, if not outright control, of the organization.

In parallel to the reactive steps often used in responding to external risks, proactively anticipating future stakeholder needs and external movement requires a more proactive approach to governance and management.

Addressing Risks and Threats

Over the last decade, agencies have begun to take the range of threats more seriously, and have pursued ways to manage and mitigate them. While government cannot eliminate all risks, agencies can put in place strategies to better plan for and manage them. Risk management is such a strategy: it is a series of coordinated activities to direct and control challenges or threats to achieving an organization's goals and objectives.

Dr. Karen Hardy, in her IBM Center report, *Managing Risk in Government: An Introduction to Enterprise Risk Management,* identifies enterprise risk management (ERM) as one tool that can assist federal leaders in anticipating and managing risks, as well as considering how multiple risks in their agency can present even greater challenges and opportunities when examined as a whole. OMB recognizes ERM as an effective agency-wide approach to addressing the full spectrum of an agency's external and internal risks. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that offers better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery. While agencies cannot respond to all risks related to achieving strategic objectives and performance goals, they must identify, measure, and assess risks related to mission delivery.

In July 2016, the OMB issued an update to OMB Circular No. A-123 requiring federal agencies to implement ERM to better ensure their managers are effectively managing risks that could affect the achievement of agency strategic objectives. OMB also updated Circular No. A-11, *Preparation, Submission, and Execution of the Budget* in 2016 and refers agencies to Circular No. A-123 for implementation requirements for ERM. The updated requirements in Circulars No. A-123 and A-11, respectively, help modernize existing management efforts by requiring agencies to implement an ERM capability coordinated with the strategic planning and strategic review process established by the GPRA Modernization Act of 2010 (GPRAMA), and with the internal control processes required by the Federal Managers Financial Integrity Act of 1982 and in our *Standards for Internal Control in the Federal Government.* This integrated governance structure can improve mission delivery, reduce costs, and focus corrective actions towards key risks.

Even before OMB required agencies to adopt ERM, some agencies implemented ERM to address risk-based issues and improve their ability to respond to future risks. The IBM Center has published reports highlighting case studies of federal agencies and their ERM efforts, such as the Office of Federal Student Aid (FSA) in the Department of Education, which adopted ERM in 2004, and the Centers for Disease Control Prevention's (CDC) RiskSmart™ credibility risk management and issues management systems. Similarly, the head of the U.S. Troubled Asset Relief Program (TARP) included risk management as a key element in ensuring performance and accountability, and a new agency head at the Defense Logistics Agency began an ERM program as a key driver for change. More recently, former Labor Department CFO Douglas Webster and former President of the Association for Federal Enterprise Risk Management highlighted how to apply ERM broadly across government in their IBM Center report, *Improving Government Decision Making through Enterprise Risk Management.*

Given the recent emphasis on addressing risks seriously, the GAO has identified six good practices that illustrate ERM's essential elements. The selected good practices are not all inclusive, but represent steps that federal agencies can take to initiate and sustain an effective ERM process, as well as practices that can apply to more advanced agencies as their ERM processes mature.

Essential Elements and Associated Good Practices of Federal Government Enterprise Risk Management (ERM)

Element	Good Practice
Align ERM process to goals and objectives *Ensure the ERM process maximizes the achievement of agency mission and results*	**Leaders Guide and Sustain ERM Strategy** Implementing ERM requires the full engagement and commitment of senior leaders, which supports the role of leadership in the agency goal setting process, and demonstrates to agency staff the importance of ERM.
Identify Risks *Assemble a comprehensive list of risks, both threats and opportunities, that could affect the agency from achieving its goals and objectives.*	**Develop a Risk-informed Culture to Ensure All Employees Can Effectively Raise Risks** Developing an organizational culture to encourage employees to identify and discuss risks openly is critical to ERM success.
Assess Risks *Examine risks, considering both the likelihood of the risk and the impact of the risk to help prioritize risk response.*	**Integrate ERM Capability to Support Strategic Planning and Organizational Performance Management** Integrating the prioritized risk assessment into strategic planning and organizational performance management processes helps improve budgeting, operational, or resource allocation planning.
Select Risk Response *Select risk treatment response (based on risk appetite), including acceptance, avoidance, reduction, sharing, or transfer.*	**Establish a Customized ERM Program Integrated into Existing Agency Processes** Customizing ERM helps agency leaders regularly consider risk and select the most appropriate risk response that fits the particular structure and culture of an agency.
Monitor Risks *Monitor how risks are changing and if responses are successful.*	**Continuously Manage Risks** Conducting the ERM review cycle on a regular basis and monitoring the selected risk response with performance indicators allows the agency to track results and impact on the mission, and whether the risk response is successful or requires additional actions.
Communicate and Report on Risks *Communicate risks with stakeholders and report on the status of addressing the risk.*	**Share Information with Internal and External Stakeholders to Identify and Communicate Risks** Sharing risk information and incorporating feedback from internal and external stakeholders can help organizations identify and better manage risks, as well as increase transparency and accountability to Congress and taxpayers.

Source: Source: GAO. | GAO-17-63

These good practices mirror many of the recommendations and approaches outlined in several IBM Center reports addressing risk management. Government experience with and insight into ERM will evolve and approaches to pursuing ERM will advance over time.

Tackling the "Internet of Threats"

From the OPM breach to the latest network penetration and hack of a private sector corporation, one of the most pressing hazards facing government agencies and governments involves cyber threats. The growing complexity and danger of the current threat environment—"Internet of Threats"—describes risks faced in moving more physical applications online, a trend magnified by the web-enablement of a broad range of applications commonly referred to as the IoT. The interconnectedness of devices today introduces technologies that connect cyber systems to physical systems. This means that potential disruptions to a system can have large and unanticipated cascading effects. Indeed, these innovations are a double-edged sword. These new technologies can also help government and industry in identifying and addressing risks and threats; in the online world, cloud-based approaches can enable instantaneous transmission of patches across a network. And artificial intelligence can automate detection of malware and mitigate risk at scale, automating routine decisions and fostering a focus on highest priorities (such as open source vulnerabilities).

At the other end of the technology scale, government continues to rely on archaic systems that retain vulnerabilities—more fundamental modernization strategies, including shared services for secure computing platforms and new technology approaches ranging from identity and access management to encryption, can reduce risk significantly. Accompanied by sound governance, agencies can adapt new technologies to support overstretched security staff who focus on results while still ensuring compliance. These experts can then address high-priority risk items even as constrained budgets remain the norm.

Given the constant threats and compliance issues that face government teams 24x7 and a world where adversaries only have to succeed once, addressing threat vectors in a risk management framework is critical. Agencies can then focus on controlling basic risks among the general population, prioritizing risks for special attention based on severity of potential threats, responding quickly to threats as they rise, and promoting resiliency in recovering from incidents that inevitably occur. A risk management framework can also enable security teams to work with mission colleagues in balancing protection relative to program impacts. This expands the focus beyond simply security, IT and systems to the people, processes, and data essential to carrying out agency goals and objectives.

Conclusion

Federal executives must understand the spectrum of risks, develop actions to mitigate risks in compliance with law and policy, and communicate risk response strategies to appropriate target populations. More importantly, assessing the inherent risks facing the public sector, and acting accordingly can drive change in government and promote successful management of government programs and missions. They need to understand and apply a set of tools and techniques and adapt them to their specific operating environment, based on best practices and lessons learned in addressing common as well as unusual risks. Risk management is not simply a compliance exercise but goes to the core of agency mission delivery.

Resources

Bullock, Justin and Robert Greer. *Risk Management and Reducing Improper Payments: A Case Study of the U.S. Department of Labor.* IBM Center for The Business of Government, 2016.

Chenok, Daniel. *Actionable Cybersecurity Practices for the 21st Century: Perspectives from Experts.* IBM Business of Government Blog, 2017.

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

Kwak, Young Hoon, and Julia Keleher. *Risk Management for Grants Administration: A Case Study of the Department of Education.* IBM Center for The Business of Government, 2016.

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

Molina, Anthony. *Ten Recommendations for Managing Organizational Integrity Risks.* IBM Center for The Business of Government, 2016.

Stanton, Thomas H. and Douglas W. Webster. *Improving Government Decision Making through Enterprise Risk Management.* IBM Center for The Business of Government, 2016.

U.S. Government Accountability Office. *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk (GAO-17-63).* 2017.

U.S. Office of Management and Budget. *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control.* 2016.

U.S. Office of Management and Budget. *OMB Circular No. A-11, Preparation, Submission, and Execution of the Budget.* 2017.