Fostering Resilient Institutions

Tools and Tactics to Manage Risks and Build Resiliency

The safety, security, and resiliency of nations and their institutions face a vast array of risks and hazards, including pandemics, malicious cyber activity, terrorism, accidents, transnational crime, fraud, natural disasters, and climate change. High impact and hard to predict events like COVID-19 reveal vulnerabilities and weaknesses in systems and across sectors. The pandemic highlighted serious weaknesses in the global supply chain, hampering government responses to life-threatening situations. When governments do respond by creating assistance programs to offset financial hardship resulting from economic impacts, these programs can increase exposure to fraud, waste, and abuse.

Crises of the past few years have underscored the need for U.S. federal agencies to strengthen and mature robust and rigorous enterprise risk management programs. In an increasingly volatile and uncertain period, agency leaders must complement these risk management efforts by inculcating resilience management approaches that go beyond event-specific business continuity or crisis management plans. Pursuing these disciplines simultaneously better positions agencies to understand acceptable risks, enabling them to redirect resources and get ahead of new and emerging threats -- building resilient organizations that can turn disruption into opportunity.

Understanding a Complex Risk Landscape

COVID-19 revealed the evolving and complex risks that government agencies confront. Yet as the pandemic recedes, this risk landscape will remain. Many risks – aging IT systems, cybersecurity threats, supply chain vulnerabilities, impacts of climate change, workforce skills gaps, or program integrity – have the potential to disrupt agency programs, mission support operations, and the ability of federal agencies to conduct the business of government. Government resilience follows from the resilience of its institutions.

The Biden-Harris administration has recognized the significance of these risks and has issued Executives Orders[1] and guidance on how agencies should manage and mitigate them. For example, the use of technologies such as social media, the Internet of Things, mobility, artificial intelligence, and cloud computing by government agencies has great benefits, but has also increased potential cyber risks. Cyberattacks against government are becoming more common and more severe – a trend made more pronounced as agencies have increased reliance on digital networks for distance work in the response and recovery efforts around COVID-19.

Technological advances have made federal agency systems, infrastructure, processes, and technologies interconnected and interdependent, such that a risk encountered in one area has the potential to cascade. Given this interconnected operational environment, managing risk across enterprises becomes s more necessary than ever. As noted in the GAO report, *Cybersecurity:*

[1] *Executive Order 14028, Improving the Nation's Cybersecurity*: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; *Executive Order 14030: Climate-Related Financial Risk,* and *Executive Order 14008*: *Tackling the Climate Crisis at Home and Abroad*

Agencies Need to Fully Establish Risk Management (GAO-19-384), cybersecurity risks must be addressed and integrated into an enterprise-wide risk management program.

Today's risk landscape requires a unified, coordinated, disciplined, and consistent approach, no longer focused on risk management as a compliance exercise or perceiving risks solely as problems to avoid. Research is needed on reconceiving risk management as a value-creating activity integral to strategic planning, decision making, and organizational resiliency. As former federal Chief Information Officer Suzette Kent so aptly notes:

> "people and operational changes due to service delivery being significantly more digital, workforce in hybrid location mode and massive growth in automation and artificial intelligence…drive the need to reexamine workforce, risk practices, and operational resiliency[2]"

The IBM Center recently launched an initiative to help governments grow more resilient in the face of increasing risks. This effort promotes research on preparing for and responding to shocks that increase in frequency and magnitude.[3]

Strengthen and Mature Enterprise Risk Management

In 2016, OMB updated Circular No. A-123, requiring federal agencies to implement enterprise risk management (ERM) to ensure agencies effectively manage risks that can potentially derail mission delivery. These flexible requirements offered agencies considerable latitude in how they set up ERM programs. This approach tied ERM to the structure, culture, and needs of each agency, avoiding the treatment of ERM as a compliance exercise[4]. IBM Center research has validated ERM as a strategy to address agency exposure to risks that impact mission, strategic goals, and operations, enabling agencies to manage risks and foster organizational resiliency.

In almost six years since the A-123 update, a growing number of agencies have implemented effective and integrated ERM programs, establishing governance, developing risk identification and assessment processes, preparing risk profiles, and improving their overall risk readiness and response--helping them better manage risks and improve decision-making. However, some agencies have not. "Progress across government has been very uneven," admits Tom Brandt, former chief risk officer at IRS and past president of Association of Federal Enterprise Risk Management (AFERM) [5], "and, in some cases, ERM programs that had gotten off to a good start, faded after leadership and organizational changes occurred."

[2] Miller, Jason. 2021. "Cyber, customer experience will continue to drive major federal technology changes", Federal News Network, December 22, 2021: https://federalnewsnetwork.com/reporters-notebook-jason-miller/2021/12/cyber-customer-experience-will-continue-to-drive-major-federal-technology-changes/

[3] https://www.businessofgovernment.org/blog/preparing-governments-future-shocks

[4] Keegan, Michael J. 2021. "Managing Enterprise Risk: Insights from Tom Brandt, Chief Risk Officer, U.S. Internal Revenue Service", *The Business of Government Magazine, Winter 2019/2020*: https://www.businessofgovernment.org/sites/default/files/Managing%20Enterprise%20Risk.pdf

[5] Brandt, Thomas. 2021. "*Federal Enterprise Risk Management Turns Five", The Business of Government Blog. July 21, 2021: https://www.businessofgovernment.org/blog/federal-enterprise-risk-management-turns-five*.

The pandemic underscored the need for continued, strengthening, maturing, and expanding of ERM across federal agencies. “Doing so”, according to Brandt, “can help ensure that we are thinking through the range of risks to agency mission, taking the steps necessary to prioritize those risks, and then acting to reduce the likelihood and impact should they occur.” But he, like many government risk professionals, sees challenges knows for programs that identify risks only to find limited support or resources to enable action.

What can research contribute to strengthen and mature ERM? First and foremost, this is a leadership imperative. The disruption of the current pandemic heightens this reality. The Partnership for Public Service in its report, *Mastering Risk: Ways to Advance Enterprise Risk Management Across Government*[6], outlines steps federal agencies should consider as a path to strengthen and mature ERM within agency operations:

- Push, don’t just pull, risk information. Rather than simply gathering risk information from core programs, add value by analyzing the information—such as for a risk appetite statement—and delivering it in a timely way to stakeholders who perform vital management and program functions.
- Increase the use of data and analytics. Use data to support an agency’s ability to identify and analyze risk, to aid stakeholder decision-making and to track the ERM program’s progress in responding to risks.
- Use technology to integrate a wider range of existing internal and external data (and move away from manual data calls in spreadsheets) to generate evidence-based risk analysis and targeted response activities that build senior leaders’ commitment to ERM
- Integrate ERM both at the enterprise and program levels. Increase integration between the ERM program and individual office risk management activities.
- Use ERM to strengthen response and future risk preparedness. ERM programs can help anticipate threats to effective crisis response—including identifying potential subsequent impacts. This could enable agencies to develop scenario-based contingency plans, test response plans and continually scan for the next emerging risk.

This last point illustrates how a complementary focus on resiliency management would benefit agencies and further embed the critical importance of strengthening and maturing risk management at the enterprise level – getting ahead of known risks offers an opportunity to build organizational resilience.

Pursuing Organizational Resiliency as a Strategic Imperative

Gartner recently identified organizational resilience as a strategic imperative, complementing the work of a fully functioning risk management program. By using ERM to provide visibility, leaders can monitor identified risks and mitigate them before they turn into disruptions or crises. DOD recognized this reality when it announced a supply chain resiliency working group to address systemic barriers limiting supply chain visibility, conduct resiliency assessments, and

[6] The Partnership for Public Service. *Mastering Risk: Ways to Advance Enterprise Risk Management Across Government.* May 26, 2020: https://ourpublicservice.org/wp-content/uploads/2020/05/Mastering-Risk.pdf.

develop effective mitigation actions. The working group will look at ways to increase visibility into the supply chain, identify risks and issues early, and implement proactive remedies.

Organizational resiliency is “the ability of an organization to resist, absorb, recover and adapt to…disruption in an ever-changing and increasingly complex environment to enable it to deliver its objectives, and rebound and prosper.[7]” Research into a strategic approach to resilience can enable agencies to go beyond simply developing business continuity and crisis management plans, which tend to be event specific. “Instead of perpetuating the illusion that we can anticipate the future, risk management should [also] try to reduce the impact of threats we don’t understand.”[8] Focusing resources in this direction positions agencies to effectively handle risks and threats that may be unknown or unlikely, but have the potential to totally disable and disrupt their operations. These sorts of risks are typically characterized as low-probability and high impact. Getting a better handle on how best to prepare and respond to them rests on a solid enterprise view of managing risk, complemented by a disciplined focus on strategic resilience management. It is about continuing to manage risks we understand, but also placing greater emphasis on establishing processes and mechanisms that can help agencies absorb unexpected system shocks and not only bounce back but bounce forward. Bouncing forward means learning from these situations and using that knowledge to strengthen capacity to respond with agility and adaptiveness.

During the pandemic, many federal agencies continued to deliver on their missions amidst uncertainty. The Internal Revenue Service distributed billions of dollars in stimulus payments to millions of individuals in only two months, and the Department of Veterans Affairs handled an almost fifteenfold increase in telehealth appointments for veterans’ physical and mental health services. These and many other agencies experimented and adapted to unprecedented demand for government services. Even DOD proved nimble enough to support large-scale telework in response to the pandemic, taking only a handful of weeks to move millions of workers into a viable and secure “work from anywhere” environment.[9] Similarly, FEMA turned crisis into opportunity by using desktop validation instead of on-site inspection to issue public assistance (PA) disaster grants; this protected workers from COVID-19 exposure and expedited the disaster grant process.[10] The Transportation Security Administration (TSA) used feedback from agents to identify the best way to protects workers; input from employees in the field now help shape future requirements for personal protective equipment (PPE), shielding and technology, to keep both passengers and officers safe[11]. These are just a handful of examples of organizational resiliency across federal agencies in the wake of the pandemic.

[7] Witty, Roberta. 2020. “Building Organizational Resilience Is a Strategic Imperative”, Gartner. August 21, 2020: https://www.gartner.com/en/documents/3989336/building-organizational-resilience-is-a-strategic-impera

[8] https://hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management

[9] Wyld, David. 2022. “The Age of Remote Work: How COVID-19 Ushered in a New Way of Working Now Transforming Organizations in Real Time”, IBM Center for The Business of Government, 2022.

[10] Datskovska, Daniella, Stacey Floam, Raymond Kulisch and Matt Lyttle. 2021. “Disaster recovery assistance in post-COVID environment: Mitigating risks of fraud while maintaining benefits of desktop validation”, Federal News Network, March 23, 2021: https://federalnewsnetwork.com/commentary/2021/03/disaster-recovery-assistance-in-post-covid-environment-mitigating-risks-of-fraud-while-maintaining-benefits-of-desktop-validation/.

[11] The Partnership for Public Service. *RESILIENT: Keeping Your Wits—Workforce, Innovation, Technology, Security—About You.* January 2021: https://ourpublicservice.org/wp-content/uploads/2021/01/Resilient.pdf.

Planning for Future Disruptions

Agencies would benefit from research on how best to engage in early warning activities to foster resiliency. Leveraging strategic foresight -- a planning tool[12] to develop the critical thinking, planning, and management competencies for considering the impact of long-term uncertainties on near-term decision making – can help. It is a necessary frame for making strategically important decisions in an increasingly complex world to reduce the risks of unanticipated consequences. It is both a mindset that keeps future impacts in mind in all decision-making, and a set of activities that aid and improve the planning processes.[13] It is important to note that foresight is not about predicting the future so much as it is identifying plausible alternative futures. Engaging in foresight works best when informed by the agency's ERM efforts. Better understanding an agency's risk profile, risk appetite, and risk registry allows leaders to identify and prepare for low-probability, high impact risks that most often test organizational resiliency.

A range of tools and techniques can help agency leadership think outside the box in exercising foresight. For example, **s**cenario planning and simulation are key tools in envisioning the future. These involve crafting multiple future scenarios to explore and learn from in terms of implications for present. actions. When engaging in these exercises key questions include:

- what programs and operations are mission critical?
- what level of disruption could be absorbed from a major event?
- At what level of disruption, would activities be temporarily or permanently impaired?
- Where is redundancy or additional support required and how can it be put in place and readied for the time when needed?

Complementing this type of planning is horizon scanning, a formal examination of information flows to identify potential threats, risks, emerging issues, and opportunities. Research here can help leaders plan for disruption, but also assist them to anticipate and prepare organizations to survive and thrive. Engaging in scenario planning and horizon scanning exercises can result in the development of playbooks that outline response programs for potential events, which support the development of resilience capabilities and justify funding such efforts.

Conclusion

The COVID-19 pandemic has demonstrated that federal agencies must continue to strengthen and mature ERM programs while also pursuing organizational resilience as a strategic imperative. It is about dedicating time and resources to create mechanisms and capacity with the goal of being better prepared for future disruptive events. As observed in the IBM Center report, *Managing The Next Crisis: Twelve Principles For Dealing With Viral Uncertainty*, governments confront a cascade of "unknown unknowns" (the category of unknowable events that tend to be the difficult ones), for which anticipatory measures can take years or decades to develop. Indeed,

[12] Greenblott, Joseph M., Thomas O'Farrell, Robert Olson, Beth Burchard. "Strategic Foresight in the Federal Government: A Survey of Methods, Resources, and Institutional Arrangements," *World Future Reviews*. December 13, 2018: https://cfpub.epa.gov/si/si_public_record_report.cfm?Lab=OSA&dirEntryId=343983.

[13] National Academy of Public Administration. *Governing with Foresight: Bringing Strategic Foresight to Bear in Policy Planning and Management*. April 12, 2016: https://napawash.org/standing-panel-blog/governing-with-foresight-bringing-strategic-foresight-to-bear-in-policy-pla.

the nation will likely face far more uncertainty in the future, making effective responses more important. This new operating reality affords government leaders an opportunity to reflect, learn, and build organizations that are more agile, adaptive, innovative, and able to mobilize swiftly and operate in new ways. Now more than ever, government leaders can take a holistic view of the managing of risk and building resiliency, prioritizing what they do know and preparing for what they don’t.