Enterprise Risk Management: A Best Practice in Managing Federal Programs

Nahla K. Ivy and Kenneth Shulman

Over the past several years, many federal agencies have applied Enterprise Risk Management (ERM) as a strategic discipline. Although the practice is still relatively new across federal government, there has been a groundswell within the federal government to adopt ERM as a best practice in managing diverse and complex programs. This federal “ERM movement” takes its cue from proven industry practices and has led to recent revisions to the policy environment around government operations.

Why ERM?

ERM differs from traditional risk management in that its value is derived from the strategic insights gained from a portfolio view of risks and opportunities, which lead to better informed decisions on agency priorities and investments. ERM moves away from siloed risk management within functional areas or individual business units, to a “system-wide” perspective on risk.

A cornerstone objective of ERM is to better inform decision-making through risk insight. This includes making calls on where to proactively manage risk and strategically pursue opportunities through a balanced perspective on risk acceptance and expected payoffs. Those payoffs may be in the form of “rewards,” for example through investment in innovative research and technology leading to scientific breakthroughs, or protection of valuable assets of the organization, such as people, property, reputation, or unique authorities.

Another motivation to pursue ERM is the desire to avoid expensive, retroactive repair to operations and reputation. While incidents cannot be avoided wholesale, an organization with an effective ERM framework is more likely to identify a developing risk and have a system to manage that risk appropriately, prior to the risk materializing in a significant way. A new risk consideration for many organizations is climate change and its impact on certain geographic areas. Several federal and state governments are seeing extreme weather occurrences, such as Hurricane Harvey in 2017 and Hurricane Sandy in 2012, happen much more frequently; ERM is a tool that governments can leverage to plan for a faster and more effective response to such events.

Lastly, ERM is a tool to inform better decision-making on resource allocation based on the priorities the organization has established. Understanding where obstacles and opportunities exist to expedite or improve government program outcomes can provide better information for decision-makers on where to invest limited resources. Tight budget environments can, in fact, be the best setting for risk-informed budget decisions.
Federal Guidance on ERM

The federal policy environment on ERM stems from the Federal Managers Financial Integrity Act (FMFIA) of 1982, which requires agency heads to provide annual assurances on the state of the overall control environment. Office of Management and Budget (OMB) provides guidance to agencies regarding implementation of FMFIA through Circular No. A-123. Reissued in July 2016 as “Management’s Responsibility for Enterprise Risk Management and Internal Control,” Circular No. A-123 restates the inherent responsibility of agencies to proactively consider and address risks through an integrated, agency-wide approach. The Circular also requires agencies to develop an agency ‘risk profile’ – an inventory of top risks that considers likely impacts to strategic, operational, reporting, and compliance objectives.

This is where traditional internal control practices meet with a renewed look at risks in all corners of the agency. OMB Circular No. A-123 requires federal agencies to integrate risk management and internal controls and highlights ERM as a best practice that agencies should strongly consider to improve accountability and effectiveness of federal programs and mission-support operations, in both financial and non-financial domains.

Similarly, in October 2016, the New York State Division of Budget issued a Bulletin requiring State agencies to prepare and submit a strategic plan, an annual performance plan and a lean process improvement plan. Additionally, the 2016-2017 Governor’s budget proposal included a requirement for each agency to develop an ERM capability.

OMB Circular No. A-11 initially established ERM as a best practice for federal government in 2015. The Circular, entitled “Preparation, Submission, and Execution of the Budget,” outlines expectations for agencies to utilize risk management practices in strategic reviews to ensure that risks are being managed in a way that can improve the agency’s performance against its stated goals.

Government ERM functions also take their cue from industry, where this integrated, holistic consideration of risks and opportunities has proven valuable to numerous organizations in terms of competitiveness, sustainability, and shareholder return. These effects are equally valuable in the government setting when translated as – enhancing agency mission achievement, organizational resilience, and benefit to taxpayers.

ERM Foundations

Effective Governance Structures Can Enable ERM

A foundational element for an effective ERM program is securing senior management buy-in regarding the value of organization-wide risk management. This can be accomplished by assigning a governing body, such as a senior level risk management committee, to oversee the program and ensure tie-in with the strategic priorities of the agency.

Risk committees can be newly established or can be integrated with existing management structures. The designated risk committee is integral in guiding the priorities of the agency’s ERM program, overseeing and performing regular reviews of the agency’s risk inventory, and informing appropriate risk mitigation strategies. The risk committee typically makes recommendations to the agency head regarding risks that require prioritization, attention, or even additional resources. The committee plays a central role in advancing the use of risk principles across the agency by championing ERM in their areas of responsibility and may also weigh in on the appropriate risk appetite for key functions or missions of the agency.

Establishing Mechanisms to Sustain ERM

Naming a Chief Risk Officer, ERM Director, or equivalent, to develop and drive the program will
allow continuous momentum behind a new ERM program. While placement of the ERM function varies in federal government, this often falls under the purview of the Chief Financial Officer or the Chief Operating Officer. In larger federal agencies, the risk officer may also oversee the agency’s performance management function, given the natural tie of risk to performance. In addition, establishing an organizational framework that includes risk reporting structures across all major business units or functions will enable top-down and bottom-up insight on risks and control deficiencies that could have impact at the agency level.

As an example at the state level, New York State Executive laws establish internal control requirements. In addition to identifying enterprise risks, entities must assess their internal controls over these risks. New York State requires agencies to conduct and report on control health at the organizational level in the agency’s annual self-assessments. ¹

Agencies will also likely need to establish new policies and directives to identify the authorities and responsibilities for management to launch and sustain new ERM programs. Agencies can do this at the parent agency level and sub-agency levels, depending on the complexity of the organization. Importantly, by designating a responsible division for ERM within the organization, such policies also can help carve out the resources needed to fund the initiative. Governments are often faced with resource limitations and competing demands on limited funds. ERM is a useful tool to guide decision-making around these resources.

Early on, an agency needs to embark on the highly collaborative work of developing a tailored ERM framework, to include a set of criteria that reflect the organization’s existing risk measures, such as those that likely already exist in the financial, security, or information technology realms. This tailored framework will serve to integrate risk information from these domains at the enterprise level, rather than attempt to replace or supersede them. Spending effort early on with internal subject matter experts in these areas will also ease adoption of the resulting ERM framework and can assist in addressing concerns about unnecessary burden or competing frameworks. This is often done through temporary working groups with representatives from multiple disciplines, including both mission and mission-support functions. In tandem with this effort, the agency should define a clear methodology for the use of those criteria, including how to identify risks, analyze them, and ultimately guide decisions on risk acceptance, mitigation, transfer, or pursuit.

ERM and Internal Controls – Complementary, not Duplicative Functions

ERM is most effective when it is applied across and through the organization. This requires a close partnership between ERM and internal control (or internal review) functions because one naturally informs the other. These functions are complementary in that significant audit findings should inform discussions on enterprise level impacts, just as agency-wide risks should inform which areas deserve a closer review or assessment of the internal control environment. For example, an internal audit finding about misuse of purchase cards could have impact at the operational level (inaccurate records) as well as at the strategic level (reputational and political damage).

Agencies pursuing this integration of ERM and internal control should expect to spend a meaningful period of time (read: years) to mature to this state. A significant amount of acculturation within the agency must typically occur in advance, to assist agency management in understanding the beneficial outcomes of applying lessons

¹ Reference: Executive Law, Article 45, Internal Control Responsibilities for State Agencies, http://public.leginfo.state.ny.us/lawssrch.cgi?NVLWO
learned from past audit findings (retrospective lens), while still enabling the agency to meet the needs of the future (prospective lens). In some cases, tying the hands of the agency based solely on past audit findings may also constrain growth and flexibility needed in the future. When in balance, this ideal state of effective information flow both vertically and horizontally across the organization is typically referred to as an “optimized” structure.

It is also important to note that despite the natural complementarity of ERM and internal control programs, each maintains differences in focus and function. ERM should remain focused on supporting strategic objectives through close partnership with senior managers and executive leaders within the organization, while the internal control function must maintain its attention on control health at the operational level. The two functions do not have to be integrated on an organizational chart, but when they communicate effectively, senior managers can gain greater insight as to the true state of the agency’s system of internal control in context of both strategic and operational risks facing the agency. Figure 1 presents a sample integrated ERM-internal control construct.

The organizational structure established for ERM and internal control groups may assist in ensuring there is partnership but not duplication of effort. The internal control function needs to ensure that it has a protected capability to provide independent reviews and assessments, while still informing management and the ERM function on the outcome of those assessments. Utilizing a common ERM framework as a mechanism to assess the impact and severity of internal control deficiencies can assist in translating whether significant deficiencies or material weaknesses present an enterprise risk. In the federal internal control environment, the definition of traditional internal control deficiencies includes impact to operations, reporting, and compliance; whereas in ERM, these considerations are important, in addition to impacts to reputation, public trust, funding, or scrutiny by oversight bodies.

**Defining Risk Appetite**

Establishing the organization’s willingness to accept risk in pursuit of its mission is an important underpinning for effective ERM. A defined risk appetite that is carried out through decisions made at both the strategic and operational levels assists an organization in ensuring that it stays within the comfort zone of senior management, but also that the organization is not excessively ‘risk averse’ in areas that are critical to mission achievement. Importantly, without a defined risk appetite, an organization may also be passing up on strategic opportunities based on an assumed risk aversion. Risk appetite is an inherent part of the context and culture of the organization.

Although it seems straightforward in concept, defining and applying risk appetite can be a fairly complex undertaking. Risk appetite statements typically identify those outcomes that should be broadly avoided or those that can be pursued with some level of acceptable failure. The language
must intentionally define areas of rigidity and flexibility. Some federal agencies have started by defining risk appetite at the highest level of the organization, while others define risk appetite in major functional areas or operational categories – for example – “in pursuit of mission, safety of people is of utmost concern and will never be compromised in favor of another objective; while in research, innovative approaches and solutions will be rewarded, despite the known potential for failure.”

Some agencies have sought to define risk appetite first in those areas where management perceives a strong misalignment in current versus ideal practices. This approach can benefit the organization by addressing “pain points” first.

Risk appetite has very clear uses for government entities that are responsible for investing, such as state pension funds. Memorializing an investment policy is a method to demonstrate risk tolerance. Accepting little to no risk will generally yield an extremely low return, whereas a high-risk investment may yield a higher return; but is the risk worth it? An agency needs to carefully weigh the benefits and risks in developing an investment policy.

The agency head ultimately establishes risk appetite and such definitions are most effective when the organization can translate the overall risk appetite to the operational level (often referred to as risk tolerance). As described in Figure 2, risk tolerance should be expressed in operational terms as to the level of acceptable variation in performance against existing metrics. For example, the organization may accept a 5% variation in timeliness metrics for a key business function, but anything beyond this should trigger closer review. Without such measures, the organization will be hard pressed to assess whether it is operating within or outside of its established risk appetite. In this environment, decisions made at the lowest level of the organization may be wildly askew from leadership’s expectations on risk taking.

Figure 2. Risk Appetite vs Risk Tolerance

Risk appetite – the amount of risk, on a broad level, an organization is willing to accept in pursuit of value.

Risk tolerance – the acceptable level of variation relative to achievement of a specific objective

- Tactical, operational
- Expressed using same metrics used to measure performance at the objective-level
- Enables measurement of the organization’s alignment with its established risk appetite

* Source: COSO, www.coso.org

Assessing Risk Appetite

How does one assess risk appetite? Agency ERM leads can survey senior management on their risk appetite perspectives through questionnaires, structured interviews, or facilitated workshops. Either method or a combination of these methods can provide critical insights into areas of alignment and misalignment in risk taking. Risk appetite typically varies by function, business process, product or service. For example, some products and services may be more integral to the organization’s mission than others and certain agency functions may have vastly different risk appetites based on what they are trying to protect or achieve. It is necessary to provide this context for senior management discussions on risk appetite and to understand where their perceived gaps in risk taking are today, versus where the organization wants to be.

Once the organization identifies the gaps, it then needs to better understand why the gaps exist and determine how to address them. This is where the hard work kicks in. Typically, these gaps reflect long-standing business practices or organizational culture that must be better understood through interviews and discussions with two key parties.
the organizational units that own and drive the business process, and the customers who receive the service. In government, for example, it is common for internal service organizations to be perceived as risk averse due to the compliance orientation of those functions. These can include mission support functions such as hiring, contracting, and legal review. Approaching these topics from the lens of the agency’s overall willingness to accept risk can refresh discussions on impacts, tradeoffs and opportunities.

To address the gaps, the ERM function can serve as a facilitator across these groups, by first understanding the constraints around a business practice (possibly regulatory or policy-based) and the opportunities (changes in policy or business practice to accept risk in limited areas) which the organization could pursue to achieve the desired performance outcomes, while remaining compliant with laws and regulations. These flexibilities can be achieved by rethinking the current business model, absorbing best practices from internal teams or peer agencies, or even via a declaration from the agency head regarding a willingness to accept more risk in targeted areas.

What is Needed to Advance ERM within an Agency?

The initial establishment of an ERM function and discipline within an agency will easily take one to two years and is highly dependent on the level of senior management buy-in and understanding of the value of ERM. Following this foundational work, the organization needs to:

• Socialize ERM principles and value proposition across management and eventually, with staff
• Emphasize management’s shared responsibility to mitigate cross-agency risks
• Pilot ERM principles in high-profile programs or projects to demonstrate the utility and value of risk disciplines to the business
• Integrate risk considerations into management decision-making on resource allocation
• Consider methods to integrate ERM principles into strategic planning, budgeting and reviews
• Define risk appetite for key functions, products, or services, including where a greater risk appetite is allowable
• Develop a partnership between ERM and internal control functions to ensure that high risk concerns translate to greater attention at the management level
• Adopt a maturity model framework against which the organization can perform regular benchmarking to assess the progress of the ERM program and integration with internal control.

Ultimately, any meaningful steps toward considering an agency’s risks and opportunities holistically, and using this insight to inform decision-making through an “eyes wide open” approach will add value and strength to the organization. In agencies with mature ERM programs, this risk insight directly informs and prioritizes decisions on resource allocation, which are intended to better serve the agency’s mission and support achievement of its stated objectives.
Author Bios

Nahla K. Ivy, MBA

Nahla K. Ivy is the Enterprise Risk Management (ERM) Officer at the National Institute of Standards and Technology (NIST), a bureau of the U.S. Department of Commerce, where she leads the bureau-wide ERM program. Prior to joining NIST, Ms. Ivy specialized in risk management and internal controls at the U.S. Department of Energy and served as a research and operations director at a corporate governance and data analytics firm.

Kenneth Shulman, CPA

Kenneth Shulman has about 40 years of auditing experience. His current role is the Assistant Comptroller for the Division of State Government Accountability of the New York State's Comptroller's Office. In this capacity, Mr. Shulman oversees the work of approximately 250 professional auditors responsible for auditing New York State government agencies, public authorities, certain New York City agencies and contractors receiving State funds. Additionally, he assists in the long-range planning for new projects.