GAO Identifies Essential Elements and Good Practices for Implementing and Sustaining Enterprise Risk Management in the Federal Government

Carole J. Cimitile, Ph.D.

Federal government leaders manage complex and inherently risky missions across their organizations, such as protecting Americans from health threats, preparing for and responding to natural disasters, building and managing safe transportation systems, advancing scientific discovery and space exploration, maintaining a safe workplace, and addressing security threats. Managing these and other complex challenges, requires effective leadership and management tools, as well as commitment to delivering successful outcomes in highly uncertain environments. While it is not possible to eliminate all uncertainties, it is possible to put in place strategies to better plan for and manage them.

Enterprise Risk Management (ERM) is 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. As such, ERM is a decision-making tool that allows leadership to view risks from across an organization's portfolio of responsibilities. ERM recognizes how risks interact (i.e., how one risk can magnify or offset another risk) and examines the interaction of risk treatments (actions taken to address a risk), such as acceptance or avoidance. For example, treatment of one risk in one part of the organization can create a new risk elsewhere or can impact the effectiveness of the risk treatment applied to another risk.

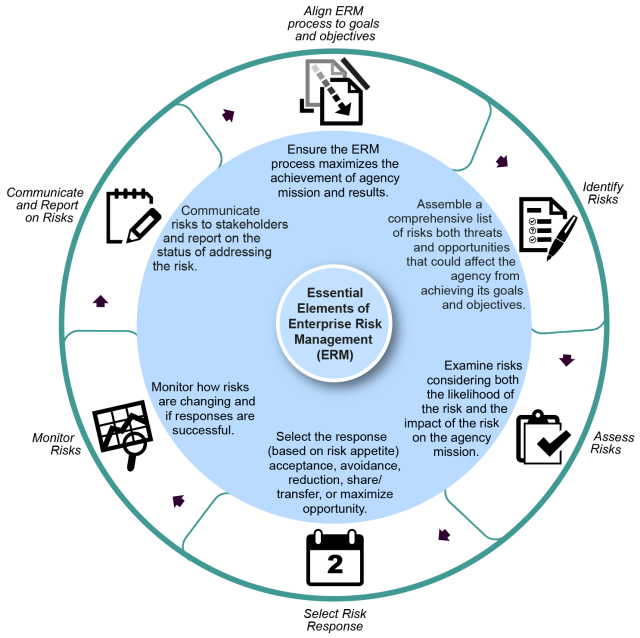
In July 2016, the Office of Management and Budget (OMB) issued an update to its Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control requiring federal agencies to implement ERM to better ensure their managers are effectively managing risks that could affect the achievement of agency strategic objectives. The updated A-123 guidance establishes management's responsibilities for ERM, as well as updates to internal control in accordance with Standards for Internal Control in the Federal Government, also known as the GAO Green Book. (See related AICPA Government Brief from October 15, 2014). Internal control is also part of ERM and used to manage or reduce risks in an organization.

Federal leaders and managers should consider ERM as part of overall organizational governance and accountability functions where an organization is exposed to risk (financial, operational, reporting, compliance, governance, strategic, reputation, etc.). An example of an agency enterprise risk is unfilled mission critical positions across the entire

organization that when examined as a whole could threaten the accomplishment of the mission.

To assist federal agencies in implementing and sustaining ERM, the U.S Government Accountability Office (GAO) issued a report, Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk, GAO-17-63, Dec. 1, 2016. See the figure below for the essential elements of ERM that GAO identified in its report. The figure below shows how ERM's essential elements fit together to form a continuing process for managing enterprise risks.

Figure 1: Essential Elements of Federal Government Enterprise Risk Management



Source: GAO. | GAO-17-63

There is no "one" right ERM framework that all organizations should adopt. However, agencies should include certain essential elements in their ERM program.

The following paragraphs describe each essential element in more detail, why it is important, and some actions necessary to successfully build an ERM program.

Align the ERM process to agency goals and objectives

Ensure the ERM process maximizes the achievement of agency mission and results. Agency leaders examine strategic objectives by regularly considering how uncertainties, both risks and opportunities, could affect the agency's ability to achieve its mission. ERM subject matter specialists confirmed that this element is critical because the ERM process should support the achievement of agency goals and objectives and provide value for the organization and its stakeholders. By aligning the ERM process to the agency mission, agency leaders can address risks via an enterprise-wide, strategically aligned portfolio view of risks rather than addressing individual risks within silos. Thus, agency leaders can make better, more effective decisions when prioritizing risks and allocating resources to manage risks to mission delivery. While leadership is integral throughout the ERM process, it is an especially critical component of aligning ERM to agency goals and objectives because senior leaders have an active role in strategic planning and accountability for results.

Identify risks

Assemble a comprehensive list of risks, both threats and opportunities, that could affect the agency from achieving its goals and objectives. This element of ERM systematically identifies the sources of risks as they relate to strategic objectives by examining internal and external factors that could affect their accomplishment. It is important that risks either can be opportunities for or threats to accomplishing strategic objectives. The literature GAO reviewed, as well as subject matter specialists, pointed out that identifying risks in any organization is challenging for employees, as they may be concerned about

reprisals for highlighting "bad news." The literature and subject matter specialists GAO consulted told us that it is important to build a culture where all employees can effectively raise risks. It is also important for the risk owner to be the person who is most knowledgeable about the risk, as this person is likely to have the most insight about appropriate ways to treat the risk.

Risks to objectives can often be grouped by type or category. For example, a number of risks may be grouped together in categories such as strategic, program, operational, financial, reporting, reputational, technological, etc. Categorizing risks can help agency leaders see how risks relate and to what extent the sources of the risks are similar. The risks are linked to relevant strategic objectives and documented in a risk register or some other comprehensive format that also identifies the relevant source and a risk owner to manage the treatment of the risk. Comprehensive risk identification is critical even if the agency does control the source of the risk.

Assess risks

Examine risks considering both the likelihood of the risk and the impact of the risk on the mission to help prioritize risk response. Agency leaders, risk owners, and subject matter experts assess each risk by assigning the likelihood of the risk's occurrence and the potential impact if the risk occurs. It is important to use the best information available to make the risk assessment as realistic as possible. Risk owners may be in the best position to assess risks. Risks are ranked based on organizational priorities in relation to strategic objectives. Agencies need to be familiar with the strengths of their internal control when assessing risks to determine whether the likelihood of a risk event is higher or lower based on the level of uncertainty within the existing control environment. Senior leaders determine if a risk requires treatment or not. Some identified risks may not require treatment at all because they fall within the agency's risk appetite, defined as how much risk the organization is willing to accept relative to mission achievement. The literature GAO reviewed and subject matter specialists noted that integrating ERM efforts with strategic planning and organizational performance management would help an organization more effectively assess its risks with respect to the impact on the mission.

Select risk response

Select a risk treatment response (based on risk appetite) including acceptance, avoidance, reduction, sharing, or transfer. Agency leaders review the prioritized list of risks and select the most appropriate treatment strategy to manage the risk. When selecting the risk response, subject matter experts noted that it is important to involve stakeholders that may also be affected, not only by the risk, but also by the risk treatment. Subject matter specialists also told us that when agencies discuss proposed risk treatments, they should also consider treatment costs and benefits. Not all treatment strategies manage the risk entirely; there may be some residual risk after the risk treatment is applied. Senior leaders need to decide if the residual risk is within their risk appetite and if additional treatment will be required. The risk response should also fit into the management structure, culture, and processes of the agency, so that ERM becomes an integral part of regular management functions. One subject matter specialist suggested that maximizing opportunity should also be included as a risk treatment response, so that leaders may capture the positive outcomes or opportunities associated with some risks.

Monitor Risks

Monitor how risks are changing and if responses are successful. After implementing the risk response, agencies must monitor the risk to help ensure that the entire risk management process remains current and relevant. The literature GAO reviewed also suggests using a risk register or other comprehensive risk report to track the success of the treatment for managing the risk. Senior leaders and risk owners review the effectiveness of the selected risk treatment and change the risk response as necessary. Subject matter specialists noted that a good practice includes continuously monitoring and managing risks. Monitoring should be a planned part of the ERM process and can involve regular checking as part of management processes or part of a periodic risk review. Senior leaders also could use performance measures to help track the success of the treatment, and if it has had the desired effect on the mission.

Communicate and Report on Risks

Communicate risks with stakeholders and report on the status of addressing the risks. Communicating and reporting risk information informs agency stakeholders about the status of identified risks and their associated treatments, and assures them that agency leaders are managing risk effectively. In a federal setting, communicating risk is important because of the additional transparency expected by Congress, taxpayers, and other relevant stakeholders. Communicating risk information through a dedicated risk management report or integrating risk information into existing organizational performance management reports, such as the annual performance and accountability report, may be useful ways of sharing progress on the management of risk. The literature GAO reviewed showed and subject matter specialists confirmed that sharing risk information is a good practice.

However, concerns may arise about sharing overly specific information or risk responses that would rely on sensitive information. Safeguards should be put in place to help secure information that requires careful management, such as information that could jeopardize security, safety, health, or fraud prevention efforts. In this case, agencies can help alleviate concerns by establishing safeguards, such as communicating risk information only to appropriate parties, encrypting sensitive data, authorizing users' level of rights and privileges, and providing information on a need-to-know basis.

GAO also identified good practices that support each particular essential element that agencies can use to support their ERM programs.

- ### 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.

- ### 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.

- ## 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.

- ## 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.

- ## Continuously Manage Risks

  Conducting the ERM review cycle on a regular basis coupled with monitoring the selected risk response with performance indicators allows the agency to track results and impact on the mission and whether the risk is successfully managed or additional actions are needed.

- ## 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.

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 be applied to more advanced agencies as their ERM processes mature. GAO expects that as federal experiences with ERM evolve, these practices will be able to be refined and additional ones will be identified.

Carole J. Cimitile, Ph.D.

Carole J. Cimitile is a senior analyst at the Government Accountability Office's (GAO) Strategic Issues Team. Carole was the analyst-in-charge of the GAO report that identified the essential elements and good practices of enterprise risk management (ERM) that federal agencies can use to implement and sustain ERM. She has also worked as a consultant helping federal agencies with program evaluation and the design and implementation of human capital policies and programs, and change management strategies.