ERM Basics for A-123

Government agencies exist to deliver service that is in the public interest. The delivery of an agency's objectives is surrounded by uncertainty which both poses threats to success and offers opportunity for increasing success. Risk is unavoidable in carrying out an organization's objectives. Lessons from the financial crisis have driven both public and private sector organizations to review and improve their risk management practices. While agencies cannot mitigate all risks related to achieving objectives and goals, they should work to the greatest extent possible to identify, measure, and assess challenges related to mission delivery so as to manage their risk to a tolerable level. Enterprise Risk Management ("ERM") is a process that allows organizations to identify, evaluate, and manage risks that could significantly disrupt the successful achievement of mission and objectives. [1]

Risk management plays an essential role in strengthening the capability to recognize, assess and address risk and capitalize on strategic opportunities. It creates a common understanding and approach. ERM is an agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM also helps agencies strengthen their capacities to evaluate alternatives, set objectives, and develop approaches to manage related risks that could compromise the achievement of strategic objectives. Moreover, the adoption of consistent risk management processes and tools can help to ensure that these risks are managed effectively, efficiently and coherently across an organization.

ERM is a distinct but complementary activity to an Agency's Internal Control processes. ERM is a strategic business discipline that addresses a full spectrum of an organization's risk. It encompasses all areas of organizational exposure to risk (financial, credit, operational, reporting, compliance, governance, strategic, reputational, etc.). Because ERM draws on an interrelated risk portfolio, it is important to understand the controls related to key organizational risks and how these controls can be used to mitigate or reduce the level of exposure to risk.

An effective ERM program will have several features:

- creates and protects value;
- is an integral part of all organizational processes;
- is part of decision-making;
- explicitly addresses uncertainty;
- is systematic, structured, and timely;
- is based on the best available information;
- is tailored and responsive to the evolving risk profile of the agency;
- takes human and cultural factors into account;
- is transparent and inclusive;
- is dynamic, iterative, and responsive to change;

[1] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management – Integrated Framework Executive Summary*, p.1

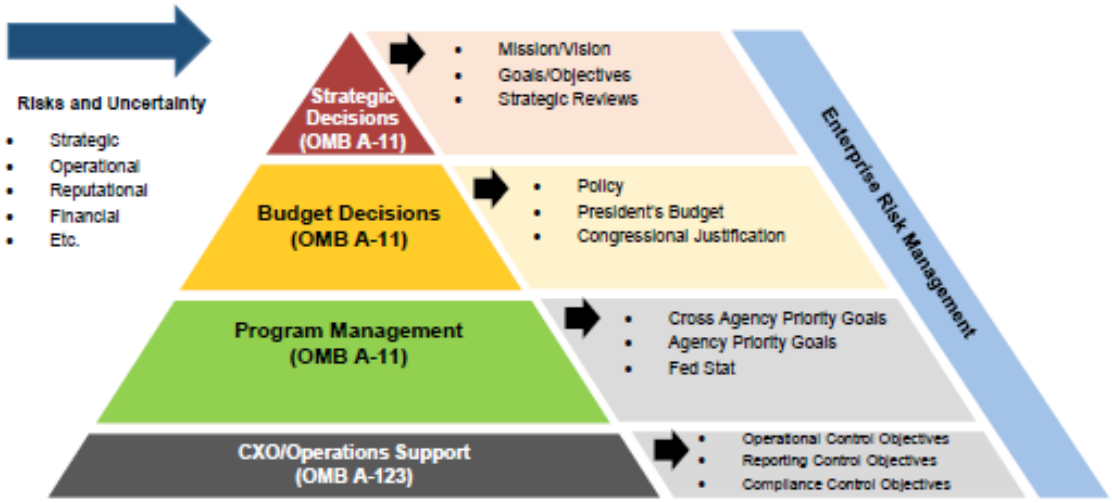
- facilitates continual improvement of the organization.

A successful ERM strategy would:

- Align goals and objectives to risk appetite
- Enhance decision-making and reduce surprises and losses
- Build capacity to respond to risk events
- Identify and manage multiple and cross-enterprise risks
- Seize opportunities

ERM Guidance

ERM guidance will be provided in a number of different places for agencies to review and decide what steps to take to implement ERM practices that are right for their agency, bureau, or department. First, OMB Circular A-123, "Management's Responsibility for Internal Control," will contain language that will provide ERM guidance for operational, reporting, and compliance control objectives. The next issuance of OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," will include language to help agencies think about incorporating ERM into their program management, budget decisions, and strategic decisions. Finally, representatives from several agencies will work together to develop an implementation guide that will provide agencies with examples of how ERM practices have been implemented across government.



ERM Governance, Culture and Basic Principles

Creating an appropriate risk culture is central to building an effective ERM program. Included in this definition of risk culture is a common understanding within the agency about the concepts, terminology, values, and attitudes toward risk. A strong culture of risk awareness at all levels of

the agency can be implemented through risk management training, risk assessments conducted collaboratively with business and program areas, agency-wide communications about the importance of sound risk identification and management, and regular reports identifying significant risks across the agency. ERM can help leaders make risk-aware decisions that impact prioritization, performance, and resource allocation.

Part of developing an agency's risk culture is to agree to basic underlying principles. These are the rules, tenets, or overarching themes that underlie the program and can be used as regular reference points to gauge whether any part of the agency is going in the desired direction.

1. **Framework is important:** ERM is built around a purposeful governance framework supported by the most senior levels of the organization and embedded in the normal working routines and activities of the agency. Agencies may choose to adopt particular standards or frameworks (for example, COSO or ISO 31000) but it is important that it be understood that there is no "one size fits all". More important than compliance with any particular standard is the ability to demonstrate that risk is managed in the particular agency, in its particular circumstances, in a way that supports good decision-making and the meeting of its objectives. Moreover, it must be forward looking with measurements concerning maturity of the ERM program along the way.

2. **Managing Risk is Everyone's Responsibility:** ERM is not about eliminating risk; it is about understanding and appropriately managing the risk inherent in our activities. All staff should be aware of the relevance of risk to the achievement of their objectives and training to support staff in risk management should be available and encouraged. Managers at each level need to be equipped with appropriate skills which will allow them to manage risk effectively.

3. **The Program/Department Owns the Risk:** This is a very basic tenet of all risk management. The managers of government activity need to own the risk of the activities they undertake. Accordingly, they need to understand, be able to articulate and (to the extent possible) manage the risk in its portfolio including risk categories of credit, market, liquidity, operational and reputational risk. If a distinct ERM department or office is created, this ERM group partners with these program/department managers to help them understand and manage their risk but it is a second line of defense.

4. **Transparency:** Informed decision making requires that we are willing to be transparent about the risks we hold or are taking. It is vital to create a culture where government employees are comfortable discussing risk openly and constructively - even when parties disagree. Part of transparency is appropriate reporting/dashboards that aggregate risk within and across silos. Moreover, the ERM culture needs to reward and not punish those that highlight risks and issues as they arise.

5. **Risk Appetite:** The amount of risk which an organization believes is tolerable and justifiable is its "Risk Appetite." Clearly expressed and well communicated risk

appetite statements can provide guidance on the amount of risk that is acceptable in the pursuit of objectives and can help policymakers make informed decisions. These statements help agencies make decisions with regard to potential consequences or impacts to other parts of the organization and can reduce surprises and unexpected losses. Risk is unavoidable in carrying out an organization's objectives. Agencies need to evaluate these risks, prioritize management of the risks, and manage the risk to a tolerable level. While agencies cannot mitigate all risks related to achieving objectives and goals, they should work to the greatest extent possible to identify, measure, and assess challenges related to mission delivery.

Risk appetite needs to be both a top down and bottom up exercise. The most senior members of an organization should be setting overall tolerable levels in conjunction with goals and objectives. It must also be considered within the context of established laws, regulations, standards, and rules. Each program must also set out individual risk appetite levels that when consolidated, are within the appetite for the entire organization.

6. **Risk Tools Can Improve Policy:** Standard risk management tools including detailed metrics and stress testing can be used to show areas where policy is working and where the goals are not being met. Effective risk management tools can sometimes help differentiate between those whose are helped and those hurt by policy, equipping agencies with the information they need to better tailor programs to specific populations and demographics. Even if the policies are not changed, this will at least help to uphold the principle of transparency. As important as risk tools can be, it is very important to understand that tools are to help inform decisions and not to make them outright. Every model has simplifications that attempt to define reality and, thus, all have imperfections. It is important to understand these imperfections and to use a number of different models and approaches where possible.

7. **Foresight planning:** Risk management needs to be forward looking, learning from past mistakes. The team will need to be able to model severe downside scenarios (and be prepared for action if need be). Moreover, we need to be able to extend our imagination to what could go wrong and be prepared for many different situations to help facilitate a "Culture of No Surprises."

8. **Forums for Discussing Risk are Important**: Forums or Committees need to exist within and across agencies for an open discussion of risk. This needs to include both leaders of the government activities and risk officers within that agency (not just risk executives speaking to each other). Lessons learned from the crisis show that it is vital to get those with different views and perspectives together to discuss issues across various businesses/agencies/programs and not just within each program/department. Committee structure will vary by agency. However, it is important that there is a mechanism in place to funnel important risk information up to the senior management of the agency or to the ultimate relevant policy maker.

9. **Diversity of People and Thought Aids Risk Management:** As discussed above, risk management is often about getting the right people around a table to discuss risk from various angles. This exercise requires diversity of thought which is greatly enhanced by diversity of people.

ERM Model Example

While each department or agency may use its own model, the example model presented here incorporates elements from the International Standards Organization (ISO) 31000: 2009 Risk Management — Principles and Guidelines; the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Integrated Framework (2004); and, the U.S. Department of Homeland Security risk management process.

1. *Establishing the Context* involves understanding and articulating the internal and external environments of the organization.
2. *Identifying Risks* involves using a structured and systematic approach to recognizing where the potential for undesired outcomes or opportunities can arise.
3. *Analyze and Evaluate* risks involves considering the causes, sources, probability the risk will occur, the potential positive or negative outcomes, and then prioritizing the results of the analysis.
4. *Develop Alternatives* involves systematically identifying and assessing a range of risk response options guided by risk appetite.
5. *Respond to Risks* involves making decisions about the best options(s) among a number of alternatives, and then preparing and executing the selected response strategy.
6. *Monitor and Review* involves the evaluation and monitoring of performance to determine whether the implemented risk management options achieved the stated goals and objectives.

7. *Communication and Learning* occurs throughout, and underpin the entire risk management process. As appropriate, risks and risk management decisions should be communicated with stakeholders, partners, and customers.