Raising the bar on managing enterprise risks

OMB’s requirements for Enterprise Risk Management in Federal Agencies

Why is there a push for Enterprise Risk Management?
Federal agencies face unprecedented risks in achieving their mission, goals, and objectives. These risks include expansion in scope of responsibilities, increased complexity in operations and technology, leadership and staff turnover, budget cuts, and a culture where employees believe they cannot report risks to leadership.

To confront this dynamic risk environment, the Office of Management and Budget (OMB) has raised the bar on risk management, directing agencies to effectively identify and manage risks using an enterprise approach.

These requirements are prescribed in the revised OMB Circular A-123 entitled, Management’s Responsibility for Enterprise Risk Management (ERM) and Internal Control released July 15, 2016. The revised Circular A-123 requires agencies to implement an ERM capability coordinated with strategic planning, budget formulation, and internal controls processes. When appropriately implemented, ERM enables greater enterprise-wide discipline and reliability to help agencies better manage risks.
What OMB expects from agencies on ERM?
OMB’s ERM guidance, which is now included in both Circulars A-11 and A-123, constitutes the ERM policy framework for the Federal government. Agencies are expected to establish a governance structure and develop a risk appetite, risk tolerances, and risk profiles. The establishment and evolution of the ERM program should be done in the context of an ERM capability maturity model.

Are ERM and internal controls the same thing?
Some believe that ERM is a redefinition or a simple modification of internal controls. The fact is ERM and internal controls are different—and agencies cannot meet the new requirements by continuing previous Circular A-123 activities.

The revised Circular A-123 clearly differentiates between ERM and internal controls by stating, “ERM is viewed as a part of the overall governance process, and internal controls as an integral part of risk management and ERM.”

Circular A-123 establishes ERM deliverables that include an ERM Implementation Approach and an annually updated Risk Profile that informs an organization’s strategy, policies, operations, and budget. These ERM efforts must be integrated with the management evaluation of internal controls (as shown below in Figure 1).

The more comprehensive nature of ERM is clear when the fundamental definitions of each are compared. Internal controls are meant to provide for effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations and audit resolution; while ERM is a discipline designed to address the full spectrum of an organization’s risks and integrates them into an enterprise-wide, strategically-aligned portfolio view.

A few tangible differences that are part of an ERM program, but not considered in internal controls, include external factors; challenges and opportunities; integration into strategic planning, performance management and budget formulation; and consideration of a broader taxonomy that considers reputation, regulatory, legislative and others factors.

Agencies that approach ERM as a simple extension of internal controls will discover that it is impossible to meet the requirements of the revised Circular A-123 and reap the benefits of ERM.
What are the benefits of ERM?
ERM can provide agencies with multiple benefits:

1. Reduces chance of crises and problems, thereby allowing leadership to focus more on mission priorities;
2. Helps protect the agency's reputation;
3. Identifies, elevates, and manages risks so that the right risks get to the right people at the right time;
4. Creates a culture where risk identification and elevation is encouraged and rewarded;
5. Builds line-of-sight into risks across organizational stovepipes to create the opportunity to leverage mitigation approaches for risks with similar root causes; and
6. Provides greater knowledge and insights into enterprise risk to improve resource allocation and strategic decision-making.

How is ERM effectively implemented?
While ERM is mature in the private sector, it is a relatively new concept in the Federal government. Agencies will likely need assistance launching ERM programs in a way that results in positive, short-term impact and sets the stage for long-term program maturation.

ERM requires knowledge, skills, and experience that goes beyond what is needed for internal controls. There are three characteristics that agencies should look for when identifying a provider of ERM services:

• A track record of implementing and maturing numerous ERM programs;
• A team with real world, front-line ERM experience; and
• Recognition among third-parties as an industry leader in ERM.

A critical lesson for both private and public organizations is that, beyond the challenges of establishing an ERM program, there are even greater and more complex challenges when integrating the program into an organization’s culture, sustaining resource commitment throughout the ERM lifecycle, and keeping it nimble enough to respond to changes in the risk environment.

Deloitte Advisory recommends a phased approach to implementing and sustaining an ERM program. Whether an agency is seeking to establish or mature an ERM program, their success will be impacted by the following factors:

• Acquiring and maintaining top leadership buy-in;
• Integrating the framework into the agency’s current risk management capabilities;
• Tailoring the framework to the agency’s mission and programs, culture, and organizational and management structure;
• Creating a culture where identification and elevation of risks is encouraged and rewarded;
• Framing ERM as a discipline to help achieve mission, not as a “gotcha” exercise; and
• Using a consistent and common framework to identify and manage risk across the agency.

For more than a decade, Deloitte Advisory’s ERM specialists have assisted over 100 clients in implementing and maturing ERM programs, including small and large Federal agencies and Fortune 250 commercial organizations. We are recognized as a leader in ERM by industry analysts, including Gartner and Kennedy Information.

Endnotes
To find out more about developing your ERM Program and Circular A-123’s requirements, contact:

Cynthia Vitters  
Managing Director  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
+ 571 424 0046  
cvitters@deloitte.com