AFERM
Association for Federal
Enterprise Risk Management

AFERM Board Expresses Concern About Growing Mischaracterization of Enterprise Risk Management in the Federal Government

In 2016, with the issuance of an update to Circular A-123, OMB set out new requirements for agencies to implement the practice of Enterprise Risk Management (ERM)[i]. ERM is not synonymous with Risk Management. However, in some instances, other purposes and roles are being ascribed to ERM that risk blurring the distinction between ERM and Risk Management. This creates confusion and undermines the unique and specific intent of ERM. The linkages and references to ERM are likely occurring because there is not a broad risk management standard or framework for government, notwithstanding those that do exist for particular risk domains such as fraud[ii] and information security[iii]. Unfortunately, as a result, ERM is becoming the defacto substitute for all manner of risk management related recommendations emanating from audit reports and other areas.

Unlike traditional risk management approaches, which tend to focus on the identification and treatment of risks in discrete functions or domains, ERM is intended to enable a "portfolio-view" of risks, looking across an organization ("the enterprise") and considering all categories of risk it may face in the delivery of its overall mission. The introduction of ERM to federal agencies was not intended to supplant or replace traditional risk management activities, rather, ERM enables the identification, assessment, and treatment of risks to the entity's mission and goals. One way it does this is by providing a mechanism for risks identified to program, process or unit level objectives to be elevated when they may individually or in the aggregate have an impact on the entity's ability to meet its mission and goals.

As shown in the figure below from OMB Circular A-123, Risk Management and Enterprise Risk Management are not the same. They are complementary disciplines undertaken as good management practices by organizations, with the outputs of Risk Management rolling up to or becoming an input to Enterprise Risk Management.

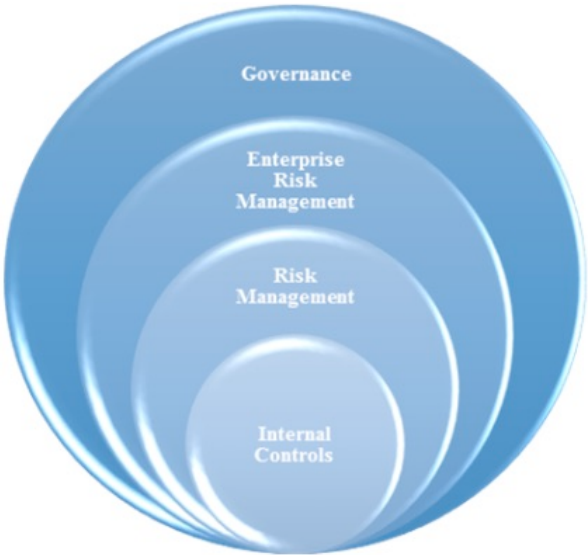

Figure 1: The Relationship between internal controls and enterprise risk management, OMB Circular A-123, pg. 8

The adoption of ERM by federal agencies was also envisioned as a means for more timely alerting senior leadership and other stakeholders of the most significant risks the agency faces in achieving its key objectives and goals while also providing insight to improve decision making.

Following issuance of the updated OMB Circular, ERM has since received growing attention and promotion through companion guides (e.g., the ERM "Playbook") as well as through conferences, training programs, and events hosted by numerous organizations, including the Association for Federal Enterprise Risk Management (AFERM). The increased awareness of ERM is helpful and desirable as it helps promote its application across government. There has also been overall healthy engagement from the oversight community, including the Government Accountability Office and several inspectors general, with multiple ERM reviews having been conducted in a manner that recognizes the overall purpose of ERM.

However, in some instances, additional purposes and roles are ascribed to ERM. This risks blurring the distinction between ERM and Risk Management, undermining the intent of ERM, and creating misperceptions about its proper use. In most cases, those seeking to ascribe other responsibilities to ERM are well-intentioned and primarily seeking to align a desired risk management outcome or practice to an existing standard. The requirement for agencies to practice ERM becomes a convenient standard to apply.

However, not all risk management is enterprise risk management, and in many cases, the recommendations being made are more appropriate for traditional risk management practices rather than ERM. For example, recommendations to "apply an ERM approach to" the identification and management of risks for a specific program, process, or activity are not appropriate as they run counter to the unique enterprise level intent of ERM.

The increased attention and awareness of the value of practicing and integrating effective risk management across government is welcome, but it is important that the distinct purpose and role for ERM remains intact. ERM, when practiced appropriately, enables a holistic and organization-wide view of the most significant risks that could impact an agency in achieving its mission. It should not be diluted into a one-size fits all or catch-all for anything risk management related in government.

To learn more about ERM, visit AFERM.org.

---

[i] OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
[ii] GAO's Framework for Managing Fraud Risks in Federal Programs
[iii] NIST Risk Management Framework for Information Systems and Organizations