J. W. Mayo
CONSULTING

jwmc-llc.com

J. W. Mayo CONSULTING

Understanding the Federal Government Risk Management Environment

joseph.mayo@jwmc-llc.com

Government ERM – OMB A-123 Introduction

Joseph W. Mayo

J. W. Mayo Consulting, LLC

joseph.mayo@jwmc-llc.com

Agenda

Introduction

Background

OMB Circular A-123

Risk Maturity Model

joseph.mayo@jwmc-llc.com

Introduction

September 12, 1950

- Public Law 784
- To authorize the President to …, to modernize and simplify governmental accounting and auditing methods and procedures, and for other purposes.

October 7, 1977

- Public Law 95-125 (P.L. 95-125)
- To amend the Accounting and Auditing Act of 1950 to provide for the audit, by the Comptroller General…

Introduction

September 8, 1982

- Federal Managers Financial Integrity Act of 1982,Public Law 97-255 (P.L. 97-255)
- An Act to amend the Accounting and Auditing Act of 1950 to require ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control of each executive agency, and for other purposes.

December 21, 2004

- Revisions to OMB Circular A-123, Management's Responsibility for Internal Control

July 15, 2016

- OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

OMB Circular A-123 at a Glance

A-123 is very good by any standard, exceptional for a Government document

Defines management's responsibilities for enterprise risk management (ERM) and internal control.

Provides updated implementation guidance to Federal managers to improve accountability and effectiveness of Federal programs as well as mission- support operations through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness.

OMB Circular A-123 at a Glance

Emphasizes the need to integrate and coordinate risk management and strong and effective internal control into existing business activities and as an integral part of managing an Agency.

Requires agencies to integrate risk management and internal control functions.

Establishes an assessment process that management must implement in order to properly assess and improve internal controls over operations, reporting, and compliance.

joseph.mayo@jwmc-llc.com

OMB Circular A-123 at a Glance

Management must evaluate the effectiveness of internal controls annually using the Green Book.

The terms “Must” and “Will” denote a requirement that management will comply with in all cases.

- There are 111 instances of ”Must”

The term “Should,” indicates a presumptively mandatory requirement

- There are 50 instances of “Should”

OMB Circular A-123 at a Glance

Agencies must identify, measure, and assess risks related to mission delivery.

Agencies must maintain a risk profile.

Risk profile must contain both positive (opportunities) and negative (threats) sources of uncertainty.

Agencies should develop a maturity model approach to the adoption of an ERM framework.

- Includes a reference to the RIMS Risk Maturity Model.

Agency governance should include a process for considering risk appetite and tolerance levels.

OMB Circular A-123 at a Glance

Requires that the head of each Executive Agency annually submit to the President and Congress a statement on whether there is reasonable assurance that the Agency's controls are achieving their intended objectives.

Primarily based on the "Green Book" and the "Orange Book".

- https://www.gao.gov/assets/gao-14-704g.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191513/The_Orange_Book.pdf

Borrowed heavily from industry (e.g. RIMS, COSO, NIST, UK Treasury).

Risk Maturity Model

J. W. Mayo CONSULTING

Five maturity levels

- Level 1: Ad hoc
- Level 2: Initial
- Level 3: Repeatable
- Level 4: Managed
- Level 5: Optimized / Industry Leader

joseph.mayo@jwmc-llc.com

Risk Maturity Model

Six primary attributes contribute to risk maturity

- ERM-based approach: This attribute focuses on the organization's risk culture and degree of executive buy-in and "tone at the top".
- ERM process management: The extent to which ERM is embedded throughout the organization's culture and the extent ERM processes are explicit, repeatable and effectively implemented.
- Risk appetite management: Focuses on the level of awareness throughout the organization of the defined risk appetite and risk tolerance.

joseph.mayo@jwmc-llc.com

Risk Maturity Model

Six primary attributes contribute to risk maturity (continued)

- Goal Alignment: Focuses on the extent risk events and opportunities are aligned with organizational goals and objectives. It also considers the degree to which performance indicators incorporate quantitative and qualitative measures.
- Risk Seeking Behavior: Focuses on the scope and breadth of risk information sources, including the extent of documentation concerning risks and opportunities.
- Business resiliency and sustainability: Evaluates the extent ERM information is used for operational planning, resilience and recovery planning, and other scenario analyses.

joseph.mayo@jwmc-llc.com

Risk Maturity Model

J. W. Mayo CONSULTING

Maturity Attribute	L1	L2	L3	L4	L5
ERM-based approach	○	●	●	●	●
ERM process management	○	◗	●	●	●
Risk appetite management		○	◗	●	●
Goal Alignment			○	●	●
Risk Seeking Behavior			○	◗	●
Business resiliency & sustainability				◗	●

● - Fully implemented throughout the Enterprise

◗ - Effectively implemented in portions of the Enterprise

○ - Inconsistent, not Enterprise-wide

joseph.mayo@jwmc-llc.com

Live Content Slide

When playing as a slideshow, this slide will display live content

Social Q&A for ISACA Maryland Chapter Virtual Conference

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Thank You!

• • •

Joseph W. Mayo

CMMI Associate, PMP, PMI-RMP, CRISC, RIMS-CRMP

joseph.mayo@jwmc-llc.com

@TaoOfRisk