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

## From 1-2-3 to E-R-M

Council of the Inspectors General on
Integrity and Efficiency
Federal Audit Executive Council
Annual Conference
September 26, 2017

# Opening Remarks

# Current Risk Environment Facing Federal Government

- The Federal government is facing greater change than at any other point in time
- Current budget realities mean government agencies compete for limited resources as never before
- Budgets will go to those who best show value
- There is greater scrutiny and expectations from internal and external stakeholders for agencies to respond to risk faster and more effectively
- The continual focus of risk management on financial areas has limited the broader considerations of risk within organizations

## Major Management Challenges

Could they have been avoided?

Could the impact have been minimized and more manageable?

*What will be next?*

# Enterprise Risk Management and Internal Control

***Risk*** is the effect of uncertainty on objectives. It is typically addressed within functional, programmatic, or organizational silos.

***Enterprise Risk Management*** is: "a discipline that addresses the full spectrum of an organization's risks, including challenges and opportunities, and integrates them into an enterprise-wide, strategically aligned portfolio view. ERM contributes to improved decision-making and supports the achievement of an organization's mission, goals, and objectives."


***Internal Control*** is a process effected by an entity's oversight body, management and personnel that provides reasonable assurance that the objectives of an entity will be achieved. (GAO Green Book)

A process to help achieve objectives (GAO Green Book)

*In other words, things you do to make sure good things happen and bad things don't.*

***Internal Control System*** is a continuous built-in component of operations, effected by people, that provides reasonable assurance, not absolute assurance, that an entity's objectives will be achieved. (GAO Green Book)

***Outcomes:***

- An increased likelihood of successfully delivering on agency goals and objectives.
- Fewer unanticipated outcomes encountered.
- Better assessment of risks associated with changes in the environment.

# Background and Context

## President's Management Agenda

***We are kicking-off a process to set the President's Management Agenda. The Administration will take action to ensure that by 2020 we will be able to say:***

**1. Federal agencies are managing programs and delivering critical services more effectively.**

**2. Federal agencies are devoting a greater percentage of taxpayer dollars to mission achievement rather than costly, unproductive compliance activities.**

**3. Federal agencies are more effective and efficient in supporting program outcomes.**

**4. Agencies have been held accountable for improving performance.**

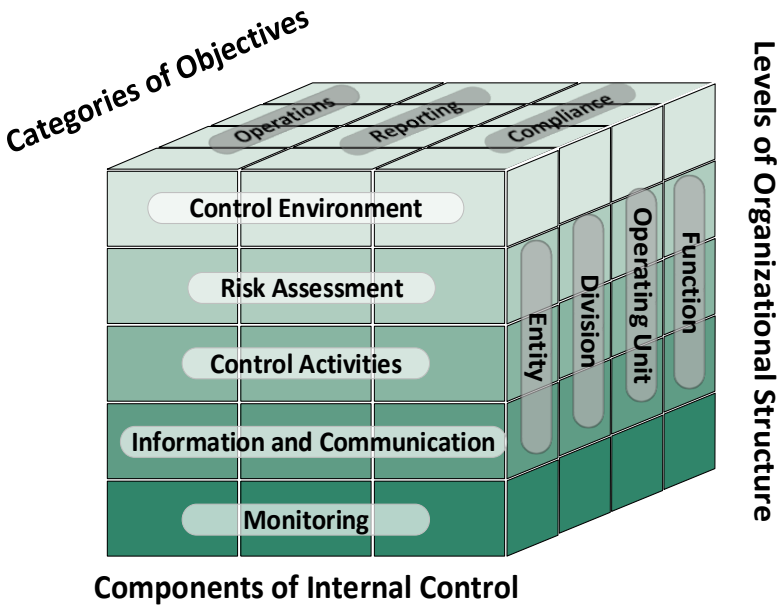
# The Decision We Made


- Compliance with New GAO Internal Control Standards
- Treating Risk as only Negative
- Heavy Emphasis on Financial Reporting
- Regarding Risk Management as Separate
- Check the Box on 3 Year A-123 Assessments

- Risk Based Approach with New Internal Control Standards
- Treating Risk as Positive (i.e., opportunity) and Negative
- Balanced Emphasis on Financial Reporting
- Integrating Risk Management and Internal Control
- Manage Risks Across Silos

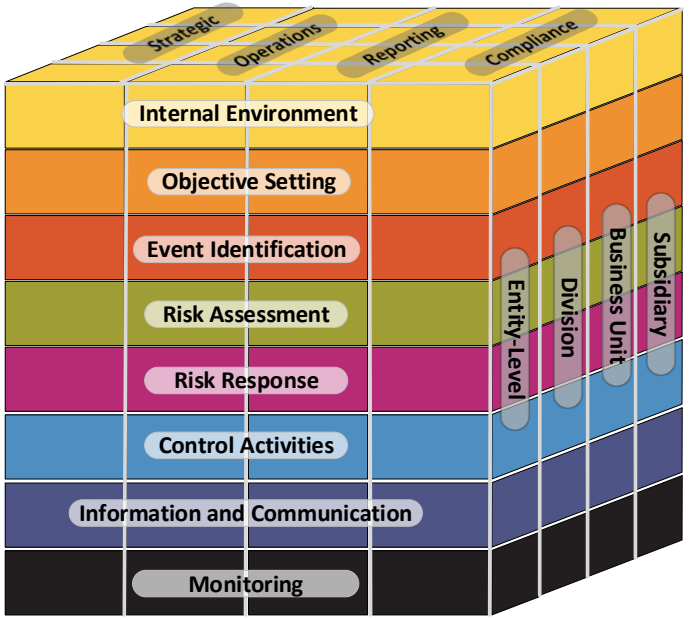
# ERM and Internal Controls The Cube Version

A-123 Section III. Update
(Internal Controls)




Source: GAO Green Book

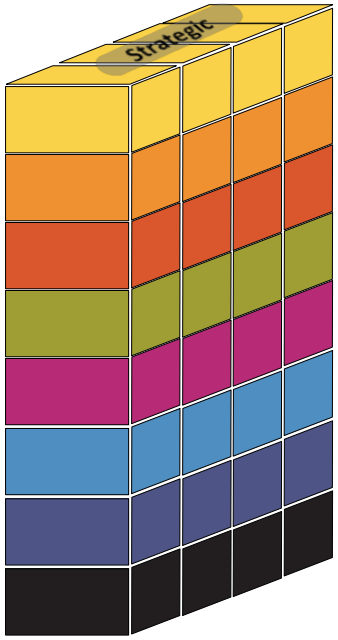
A-123 Section II. Update
(Enterprise Risk Management)




Source: Based on COSO

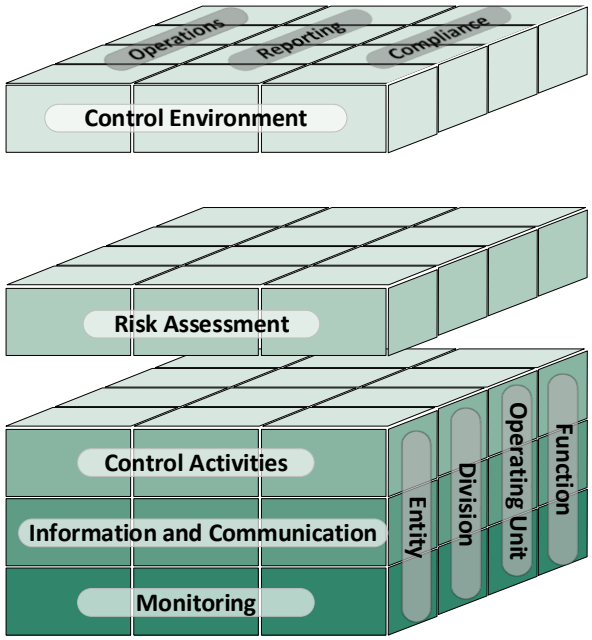
# Expanding on the Green Cube To Include ERM

## 2017 Requirements to A-123, Incorporating Strategic Objectives



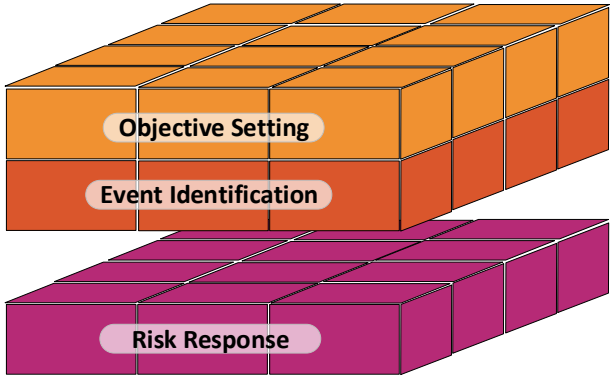

The inclusion of a strategic process to risk management and internal control

## 2016 Update to A-123, Internal Controls




The organization of internal controls as introduced in the 2014 Green Book

## 2017 Requirements of A-123, Expansion of Risk Assessment




The introduction and refinement of ERM components to be integrated into existing internal control processes

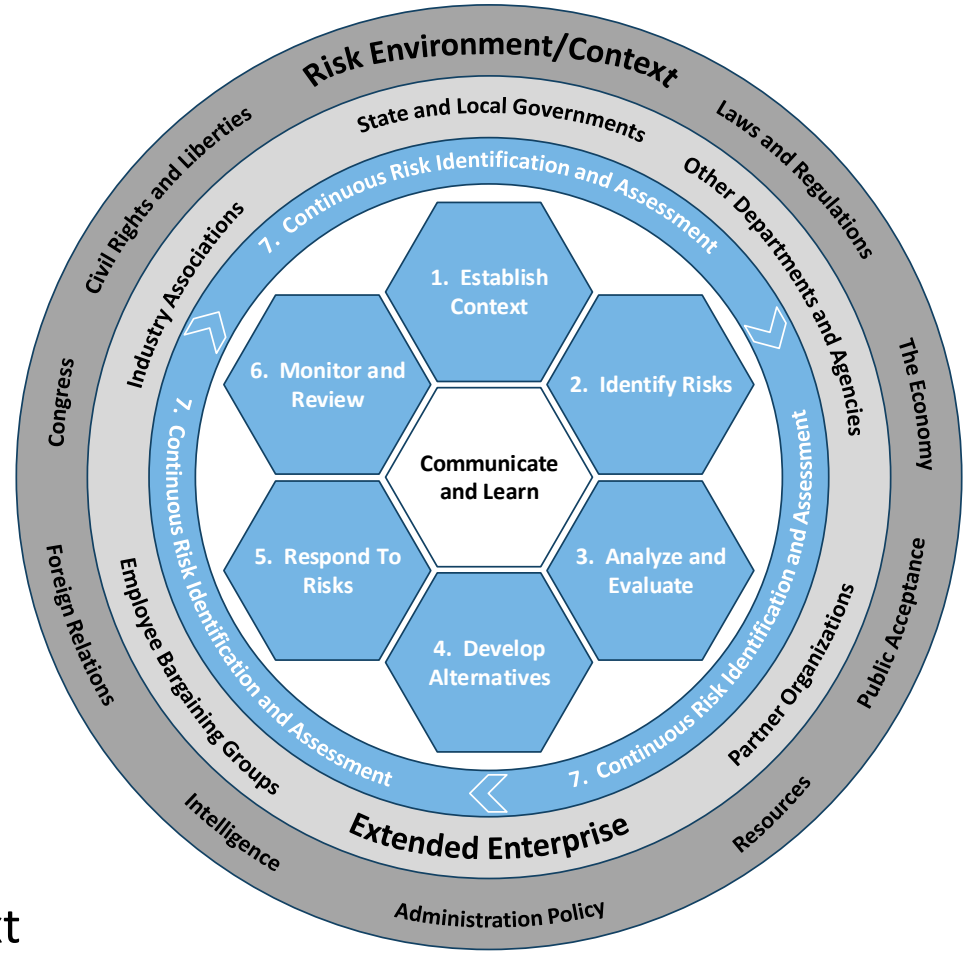
# Enterprise Risk Management Model

**Overview:**

- **7 Cyclical Components**
  - Establish the Context
  - Identify Risks
  - Analyze and Evaluate
  - Develop Alternatives
  - Respond to Risks
  - Monitor and Review
  - Continuous Risk Identification and Assessment

- **3 Enterprise Components**
  - Communicate and Learn
  - Extended Enterprise
  - Risk Environment/Context

***Illustrative Example of an Enterprise Risk Management Model***



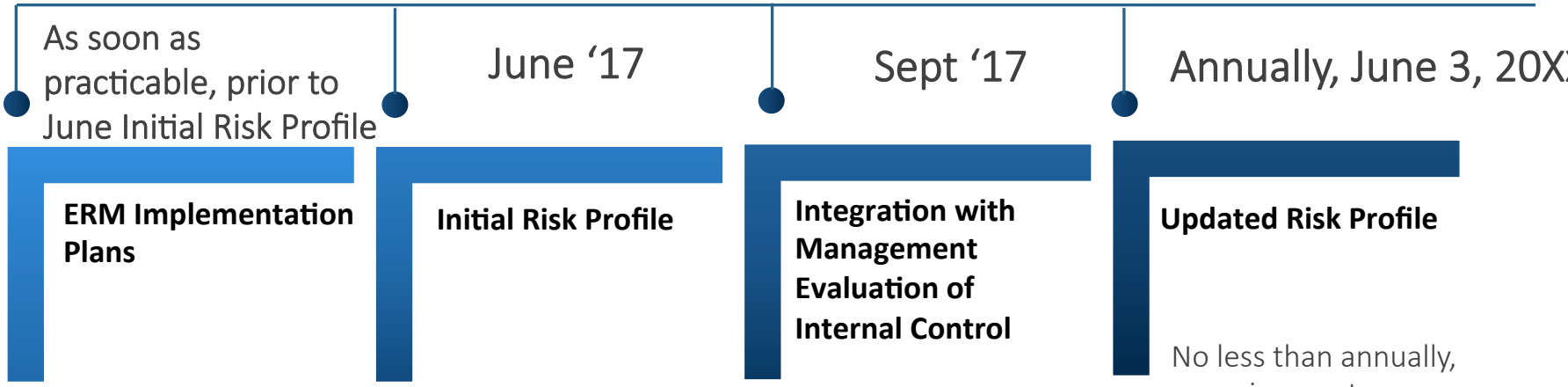
# What Is Required by A-123 to Implement ERM?

- Governance: Agencies must establish an ERM governance structure.
  - Agencies have discretion and flexibility in overall governance structure.
  - Should be led by high ranking policy official, COO or equivalent.
  - Agencies may establish a Chief Risk Officer, but are not required to.
  - Should include a process for considering risk appetite and risk tolerance.

- Risk Profiles: Establish a **"risk profile"** with the following components:
  - Identification of Objectives
  - Identification of Risk
  - Inherent Risk Assessment
  - Current Risk Response
  - Residual Risk Assessment
  - Proposed Risk Response
  - Proposed Risk Response Category


- Integration: Risk profiles to be integrated with management evaluation of Internal Control (Reasonable Assurance Process)

# Revised OMB Circular A-123
# ERM Implementation




Agencies are encouraged (not required) to develop an approach to implement Enterprise Risk Management.

Agencies must complete their initial risk profiles in coordination with the agency Strategic Reviews. Key findings should be made available for discussion with OMB as part of the Agency Strategic Review meetings and/or FedSTAT.

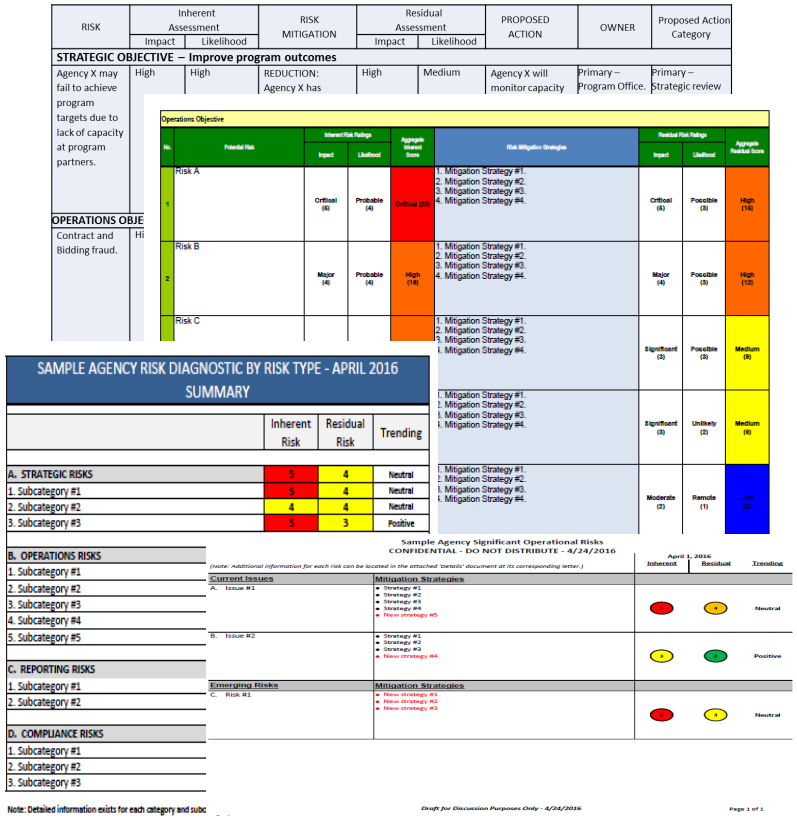
For those risks for which formal internal controls have been identified as part of the Initial Risk Profile in FY 2017, assurances on internal control processes must be presented in the Agency FY 2017 Annual Financial Report (AFR) or Performance and Accountability Report (PAR).

No less than annually, agencies must prepare a complete risk profile and include required risk components and elements required by this guidance. CFO Act Agencies, at a minimum, must complete their risk profiles in coordination with the agency Strategic Review. For these Agencies, key findings should be made available for discussion with OMB by June 3rd as part of the Agency Strategic Review meetings and/or FedSTAT.

# Creating an Enterprise-Level Risk Profile

**Agencies have discretion in terms of content and format for their Risk Profiles**; however, in general risk profiles should include the following components:

- Identification of Objectives
- Identification of Risk
- Inherent Risk Assessment
- Current Risk Response
- Residual Risk Assessment
- Proposed Risk Response
- Proposed Risk Response Category



| RISK | Inherent Assessment | | RISK MITIGATION | Residual Assessment | | PROPOSED ACTION | OWNER | Proposed Action Category |
|---|---|---|---|---|---|---|---|---|
| | Impact | Likelihood | | Impact | Likelihood | | | |
| **STRATEGIC OBJECTIVE – Improve program outcomes** | | | | | | | | |
| Agency X may fail to achieve program targets due to lack of capacity at program partners. | High | High | REDUCTION: Agency X has | High | Medium | Agency X will monitor capacity | Primary – Program Office. | Primary – Strategic review |
| **OPERATIONS OBJE** | | | | | | | | |
| Contract and Bidding fraud. | Hi | | | | | | | |

Operations Objective

| No. | Potential Risk | Inherent Risk Ratings: Impact | Inherent Risk Ratings: Likelihood | Aggregate Inherent Score | Risk Mitigation Strategies | Residual Risk Ratings: Impact | Residual Risk Ratings: Likelihood | Aggregate Residual Score |
|---|---|---|---|---|---|---|---|---|
| 1 | Risk A | Critical (4) | Probable (4) | Critical (16) | 1. Mitigation Strategy #1.<br>2. Mitigation Strategy #2.<br>3. Mitigation Strategy #3.<br>4. Mitigation Strategy #4. | Critical (4) | Possible (3) | High (16) |
| 2 | Risk B | Major (4) | Probable (4) | High (16) | 1. Mitigation Strategy #1.<br>2. Mitigation Strategy #2.<br>3. Mitigation Strategy #3.<br>4. Mitigation Strategy #4. | Major (4) | Possible (3) | High (12) |
| | Risk C | | | | 1. Mitigation Strategy #1.<br>2. Mitigation Strategy #2.<br>3. Mitigation Strategy #3.<br>4. Mitigation Strategy #4. | Significant (3) | Possible (3) | Medium (9) |
| | | | | | 1. Mitigation Strategy #1.<br>2. Mitigation Strategy #2.<br>3. Mitigation Strategy #3.<br>4. Mitigation Strategy #4. | Significant (3) | Unlikely (2) | Medium (6) |
| | | | | | 1. Mitigation Strategy #1.<br>2. Mitigation Strategy #2.<br>3. Mitigation Strategy #3.<br>4. Mitigation Strategy #4. | Moderate (2) | Remote (1) | Low (2) |

**SAMPLE AGENCY RISK DIAGNOSTIC BY RISK TYPE - APRIL 2016 SUMMARY**

| | Inherent Risk | Residual Risk | Trending |
|---|---|---|---|
| A. STRATEGIC RISKS | 5 | 4 | Neutral |
| 1. Subcategory #1 | 5 | 4 | Neutral |
| 2. Subcategory #2 | 4 | 4 | Neutral |
| 3. Subcategory #3 | 5 | 3 | Positive |
| B. OPERATIONS RISKS | | | |
| 1. Subcategory #1 | | | |
| 2. Subcategory #2 | | | |
| 3. Subcategory #3 | | | |
| 4. Subcategory #4 | | | |
| 5. Subcategory #5 | | | |
| C. REPORTING RISKS | | | |
| 1. Subcategory #1 | | | |
| 2. Subcategory #2 | | | |
| D. COMPLIANCE RISKS | | | |
| 1. Subcategory #1 | | | |
| 2. Subcategory #2 | | | |
| 3. Subcategory #3 | | | |

Note: Detailed information exists for each category and subc

Sample Agency Significant Operational Risks
CONFIDENTIAL - DO NOT DISTRIBUTE - 4/24/2016

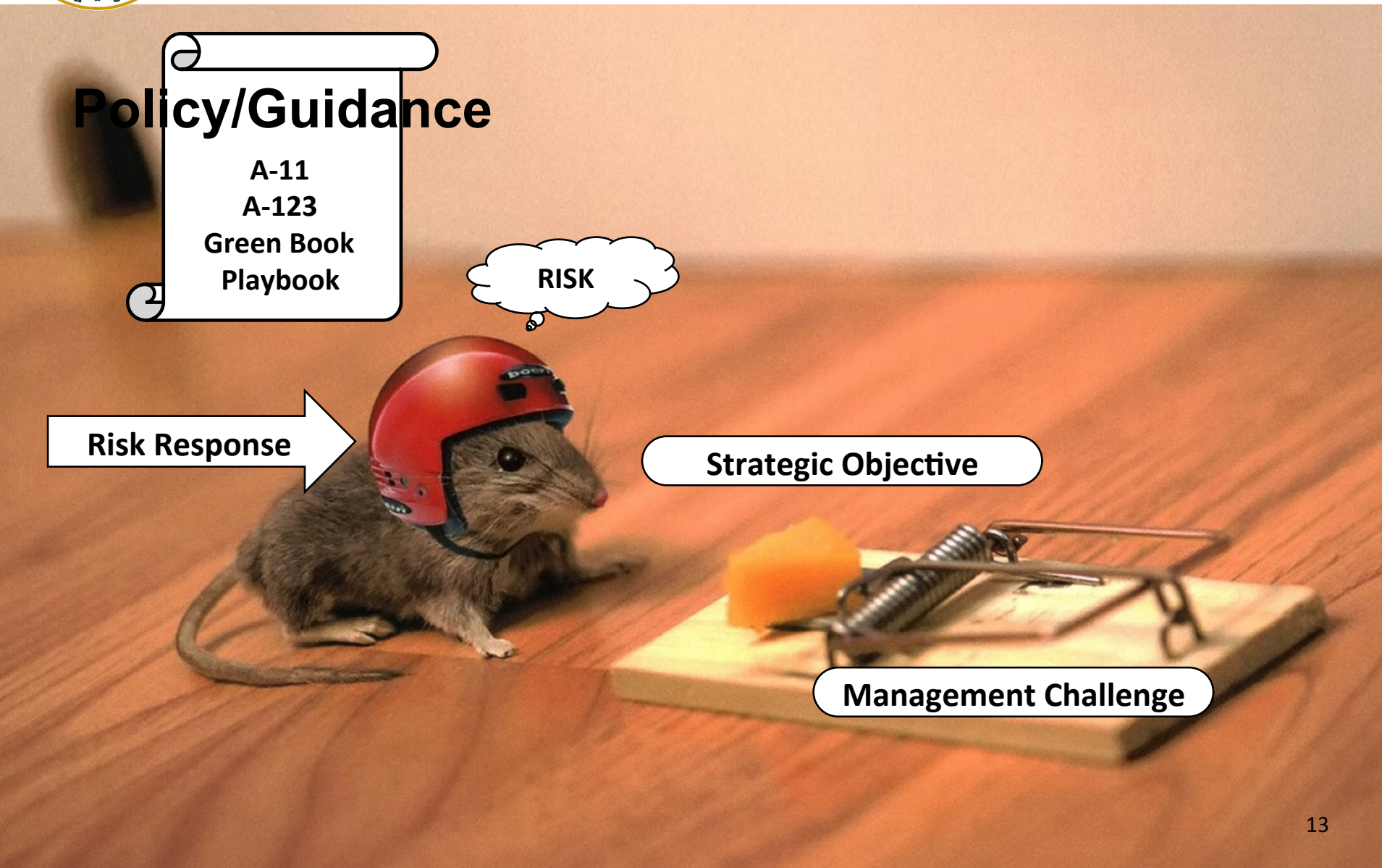
(Note: Additional information for each risk can be located in the attached 'details' document at its corresponding letter.)

| | | April 1, 2016 Inherent | Residual | Trending |
|---|---|---|---|---|
| Current Issues | Mitigation Strategies | | | |
| A. Issue #1 | ▪ Strategy #1<br>▪ Strategy #2<br>▪ Strategy #3<br>▪ Strategy #4<br>▪ New strategy #5 | 5 | 4 | Neutral |
| B. Issue #2 | ▪ Strategy #1<br>▪ Strategy #2<br>▪ Strategy #3<br>▪ New strategy #4 | 5 | 3 | Positive |
| Emerging Risks | Mitigation Strategies | | | |
| C. Risk #1 | ▪ New strategy #1<br>▪ New strategy #2<br>▪ New strategy #3 | 5 | 4 | Neutral |

Draft for Discussion Purposes Only - 4/24/2016

Page 1 of 1

# Risk Profile: An Illustrative Example



# Chief Risk Officer (CRO)

# ERM Key Terminology

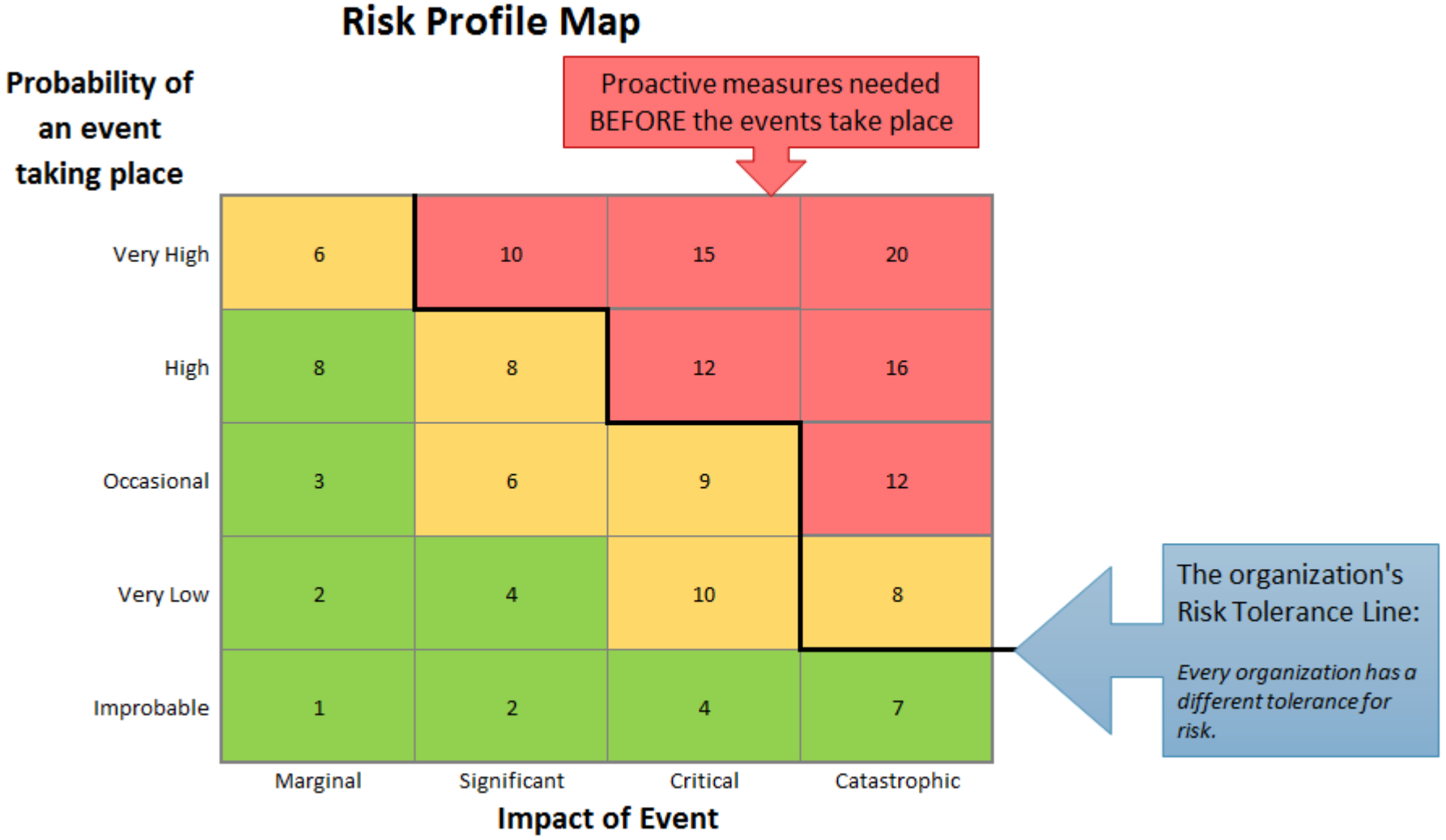
## Risk Appetite

"The broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives."

## Risk Tolerance

"The acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite."

# Heat Map – Illustrative Example



# ERM Key Terminology

- Portfolio View of Risk

"Provides insight into all areas of organizational exposure to risk (such as reputational, programmatic performance, financial, information technology, acquisitions, human capital, etc.), thus increasing an Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment."

# ERM Implementation Playbook

**Playbook Purpose:** To provide an ERM Framework and practical guidance to support A-123 compliance and effective ERM implementation across agencies.

**ERM Playbook Steering Committee**
*Set project policy and established the timeline for the project.*

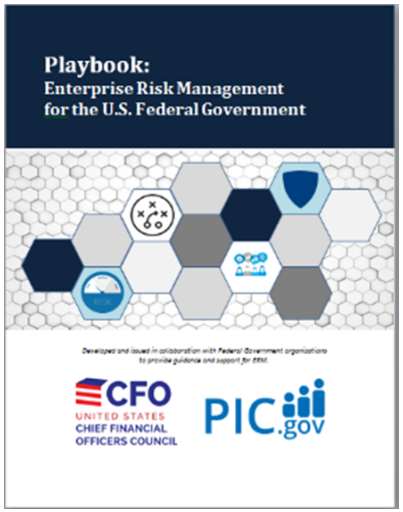
⇔

**ERM Playbook Working Group**
*Implemented the project goals set by steering committee and keyed up decisions and recommendations for the Steering Committee.*

Multi-disciplinary representation from across the federal government

- ✓ Financial Management
- ✓ Procurement
- ✓ Risk Management
- ✓ Internal Controls
- ✓ Human Capital
- ✓ IT
- ✓ Performance Management
- ✓ Grants Management
- ✓ Federal Credit

Over twenty federal agencies represented

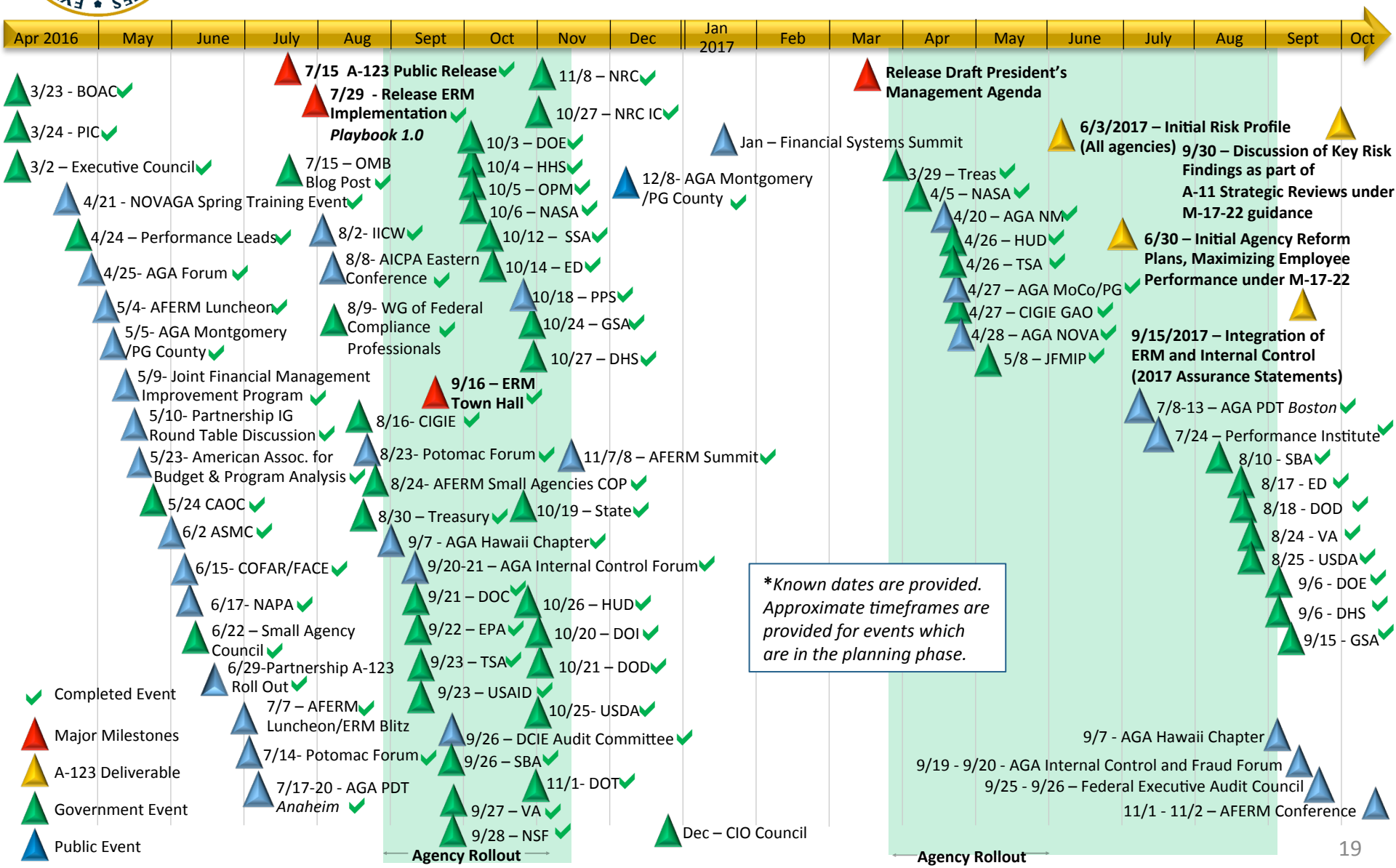



Access the Playbook at these websites

CFO Council: www.cfo.gov

AFERM: www.aferm.org

# OMB Circular A-123 and Playbook Outreach Efforts and Major Milestones



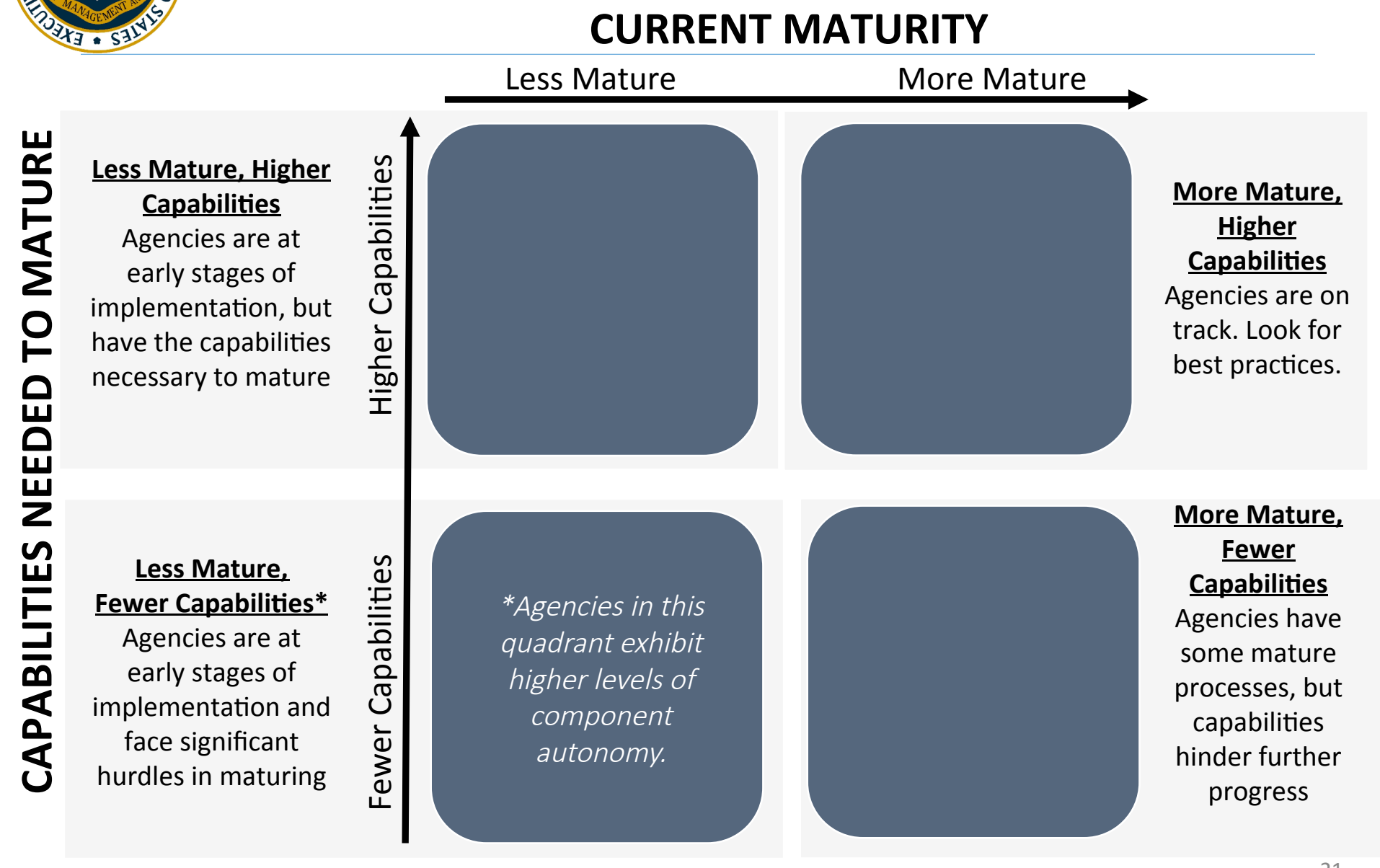
# ERM - Key Factors

**Leadership**

**Process**

**Culture**

# A-123/ERM Assessments

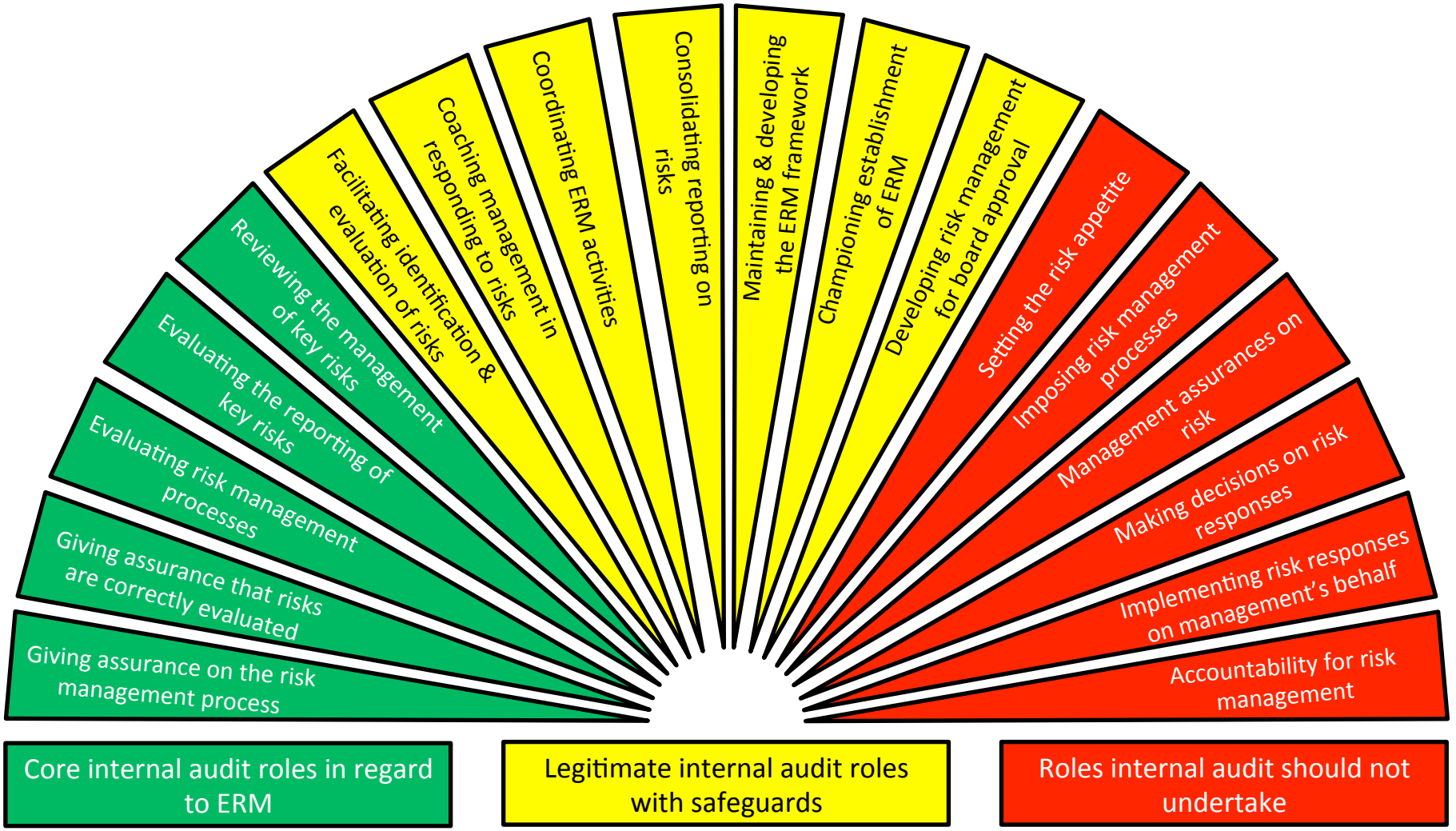


# A New Set Of Parameters
# Towards a More Resilient Government

- "**Successful implementation** of this Circular requires Agencies to establish and foster an **open, transparent culture** that encourages people to **communicate** information about **potential risks** and other concerns with their superiors **without fear of retaliation or blame**.
- "Similarly, **agency managers, Inspectors General (IG) and other auditors** should establish a **new set of parameters** encouraging the **free flow of information** about agency risk points and corrective measure adoption."
- "An **open and transparent culture** results in the earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a **more resilient government**."

-- OMB Circular No. A-123

# ERM and the Role of the Auditor




Source: Based on IIA model for internal audit role with ERM

# Core Internal Audit Roles in Regard to ERM


**Evaluating and Reviewing Established Risk Processes**

- Evaluating the agency's established risk management processes.
- Evaluating the agency's efforts at reporting on key risks.
- Providing assurances on the agency's risk management processes.

Source: Based on IIA model for internal audit role with ERM

# Roles Internal Audit Should Not Undertake


Active Management and Ownership Over ERM

- Making decisions and actions typically in the purview of management.
- Taking responsibility for risk decisions and responses
- Giving assurances for ERM and risk responses.

Source: Based on IIA model for internal audit role with ERM

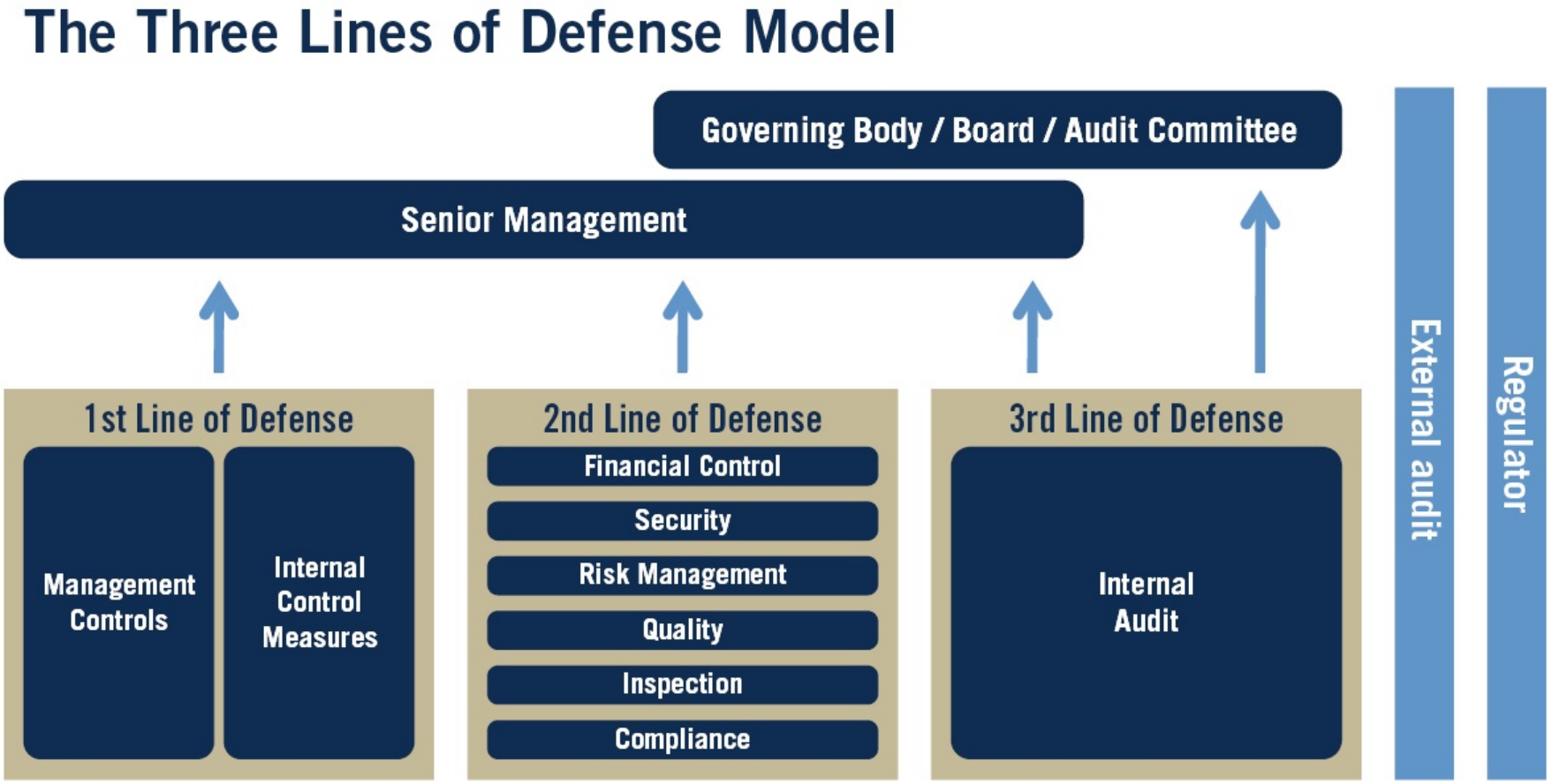
# Legitimate Internal Audit Roles With Safeguards


Assisting and Improving ERM Development

- Advocating ERM as a good management tool.
- Working with management to identify, evaluate, respond to risks
- Coordinating with management to develop and improve ERM frameworks

Source: Based on IIA model for internal audit role with ERM

# ERM and the Role of the Auditor

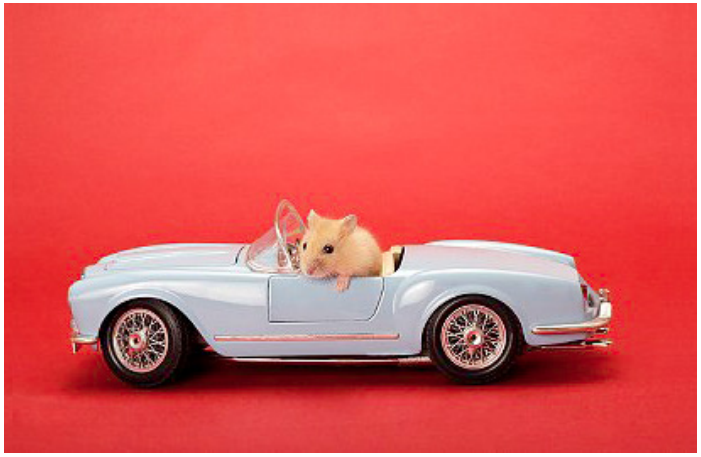



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

# Why Do Cars Have Brakes?

- "Why does a car have brakes? A car has brakes so it can go ***fast***. If you got into a car and you knew there were no brakes, you'd creep around very slowly. But if you have brakes you feel quite comfortable going 65 miles an hour down the street. The same is true of [risk] limits."

-- John Reed, former CEO of Citigroup to the Financial Crisis Inquiry Commission



# Questions?

# More Questions?

Please Contact
Office of Federal Financial Management (OFFM)
Performance and Personnel Management (PPM)
Dan Kaneshiro, Daniel_S_Kaneshiro@omb.eop.gov
Mark Bussow, Mark_Bussow@omb.eop.gov