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.

---

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

- **Governance:** Agencies must establish a 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 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)
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 Profile: An Illustrative Example

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
Maturity Model

Level 1
Ad hoc

Level 2
Preliminary

Level 3
Defined

Level 4
Integrated

Level 5
Optimized

A-123/ERM Assessments

CURRENT MATURITY

Less Mature, Higher Capabilities
Agencies are at early stages of implementation, but have the capabilities necessary to mature

Less Mature, Fewer Capabilities
Agencies are at early stages of implementation and face significant hurdles in maturing

More Mature, Higher Capabilities
Agencies are on track. Look for best practices.

More Mature, Fewer Capabilities
Agencies have some mature processes, but capabilities hinder further progress
A-11: The Next Step Building out ERM

ERM Driving Risk Informed Decisions
Addressing Risk as Part of Strategic Reviews

After the passage of the GPRA Modernization Act, OMB established annual Strategic Reviews. These reviews are an annual assessment which synthesizes broad sources of evidence to inform budget, legislative, and management decisions.

- One of the priority maturity areas is to better manage risks to goal achievement.

Components of a Strategic Review

Integration with Strategic Reviews

Agencies must update their 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.

Integration with Management Evaluation of Internal Control

For those risks for which formal internal controls have been identified and linked to the Risk Profile in FY 2018, assurances on internal control processes must be presented in the Agency FY 2018 Annual Financial Report (AFR) or Performance and Accountability Report (PAR).

Updated Risk Profile

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 update their risk profiles in coordination with the agency Strategic Review. For these Agencies, key findings should be made available for discussion with OMB as part of the Agency Strategic Review meetings.
How Can Agencies do this?

- Key themes for integrating ERM into the Strategic Review process:

  - Ensuring the risk profile is incorporated into the strategic review process
  - Engaging the right stakeholders in the strategic review process
  - Defining the missed opportunities of not including the risk profile

A-123 Restructured

A-123 Before

- OMB Circular 123/Appendix A
  - Financial Reporting
    - Appendix B, Charge Cards
    - Appendix C, Improper Payments
    - Appendix D, Financial Systems

A-123 2016-2018 Updates

- OMB Circular A-123
  - Enterprise Risk Management and Internal Control
    - Appendix A, Reporting
    - Appendix B, Charge Cards
    - Appendix C, Improper Payments
    - Appendix D, Financial Systems

A-123 Future (Proposed)

- OMB Circular A-123
  - Enterprise Risk Management and Internal Control
    - Appendix A, Reporting and Data Integrity Risk
    - Appendix B, Charge Card Misuse Risk
    - Appendix C, Payment Integrity Risk
    - Appendix D, Financial System Integrity Risk
### Internal Control Over Financial Reporting

#### Financial

<table>
<thead>
<tr>
<th>Objectives May Relate to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The President’s Budget</td>
</tr>
<tr>
<td>Agency Financial Reports</td>
</tr>
<tr>
<td>USA Spending</td>
</tr>
<tr>
<td>Payment Accuracy</td>
</tr>
</tbody>
</table>

#### Non-Financial

<table>
<thead>
<tr>
<th>Objectives May Relate to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Control Reviews and Reports</td>
</tr>
<tr>
<td>Performance &amp; Accountability Reports</td>
</tr>
<tr>
<td>Custody of Assets</td>
</tr>
<tr>
<td>USA Spending</td>
</tr>
<tr>
<td>Research and Development Reports</td>
</tr>
</tbody>
</table>

#### Characteristics

<table>
<thead>
<tr>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statutory Requirements</td>
</tr>
<tr>
<td>Transparency (FOIA)</td>
</tr>
<tr>
<td>Accountability</td>
</tr>
</tbody>
</table>

#### Internal Financial Reporting Objectives

<table>
<thead>
<tr>
<th>May Relate to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Financial Reports</td>
</tr>
<tr>
<td>Components/Bureau/Program Reports</td>
</tr>
</tbody>
</table>

#### Internal Non-Financial Reporting Objectives

<table>
<thead>
<tr>
<th>May Relate to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benchmarking/FedStat</td>
</tr>
<tr>
<td>Staff/Asset Utilization</td>
</tr>
<tr>
<td>Customer Satisfaction Measures</td>
</tr>
<tr>
<td>Real Property/Space Utilization</td>
</tr>
</tbody>
</table>

---

The proposed Expansion from External, Financial Reporting (ICOFR) to Include all Internal Control Over Reporting (ICOR) was already accomplished through the update to A-123, introduction of ERM. Agencies must manage risk to reporting objectives.

---

### 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

---
More Questions?

Please Contact
Office of Federal Financial Management (OFFM)
Performance and Personnel Management (PPM)
Dan Kaneshiro, Daniel_S_Kaneshiro@omb.eop.gov
Adam Lipton, Adam_S_Lipton@omb.eop.gov
Appendix
Proposed Updates A-123, Appendices A-B-C-D

- Restructure A-123 Appendices A, B, C and D to illustrate management’s responsibility for managing risk in key programs that relate to an agency’s strategic, operations, reporting and compliance objectives and to go beyond internal controls.
  - Appendix A: Internal Control Over Financial Reporting to Reporting and Data Integrity Risk
  - Appendix B: Charge Cards to Charge Card Misuse Risk
  - Appendix C: Improper Payments to Payment Integrity Risk
  - Appendix D: Financial Systems to Systems Risk
- Realignment and integration with ERM Processes in A-123
  - Alignment with risk management concepts and guidance.
  - Realignment for integration of A-123 risk profiles.
  - Emphasis on managerial discretion in managing risk
  - Update guidance for internal control systems consistent with the new GAO Green book.
- Realignment of requirements to achieve burden reduction
  - Realignment of A-B-C-D to become less proscriptive, mandatory guidance, more “Appendices” of best practices.
  - Clarify language to indicate Mandatory requirements (Must), Presumptive Mandatory Requirements (Should) become Best Practices (May).

Federal Performance Framework

- Goal Pipeline
  - Cross-Agency Priority Goals
    - Mission-focused
    - Management
- Strategic Goals
  - Strategic Objectives
  - Agency Priority Goals (APGs)
- Performance Goals

Planning
- Every 4 yrs.
- Annually
- Quarterly
- Federal Performance Plan
- APG Action Plan Updates
- Agency Strategic Plan
- Annual Performance Plan

Evidence, Evaluation, Analysis, and Review
- Quarterly
- Annually
- APG Goal Reviews
- APG Quarterly Reviews

Reporting
- Quarterly
- Annually
- APG Goal Progress Updates
- APG Quarterly Progress Updates
- Annual Performance Report

Management feedback
Stakeholder feedback
Decision-making and Learning to Improve Outcomes and Productivity
Operational, policy, and budget decisions, and updates to plans including milestones and improvement actions
ERM Implementation w/ the Federal Performance Framework and Strategic Review Timeline

The “Strategic Review”

- **Winter**
  - **Agency Methodology Developed**
    - Agencies develop a method to assess progress
    - OMB reviews method

- **Spring**
  - **Agency Conducts Review**
    - Agencies assess each objective
    - Agency leaders determine proposed changes to operations and strategies or budget and legislative proposals

- **May**
  - **OMB Engagement**
    - Agencies provide OMB a “summary of findings” from their review for deliberation
    - OMB provides feedback and priorities for policy and budget development

- **Sept.**
  - **Agency Submission**
    - Agency budget and performance submissions incorporate findings and OMB feedback

- **Feb.**
  - **Publication**
    - Annual Performance Report includes findings and Performance Plan proposes improvement actions
    - President’s Budget reflects key proposals

Chief Risk Officer (CRO)

- **CAO Organization**
  - High Risk
  - Medium Risk
  - Low Risk

- **PIO Organization**
  - Medium Risk

- **CFO Organization**
  - Low Risk

- **HR Organization**
  - Medium Risk

- **Chief Risk Officer**
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.”

---

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.”
Risk Heat Map

Risk Profile Map

<table>
<thead>
<tr>
<th>Probability of an event taking place</th>
<th>Marginal</th>
<th>Significant</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>6</td>
<td>10</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>High</td>
<td>8</td>
<td>8</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>Occasional</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Very Low</td>
<td>2</td>
<td>4</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>Improbable</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

The organization’s Risk Tolerance Line: Every organization has a different tolerance for risk.

Illustrative Governance Structure

Board
- Consultation and Outreach Committee
- Technology Committee
- Finance Committee
- Governance and Personnel Committee
- 

CEO SAT Chair

Senior Assessment Team (SAT)
- Strategic
- Operations
- Reporting
- Compliance

Internal Control Core Assessment Team (CAT)
- Strategic
- Operations
- Reporting
- Compliance

Risk Management Team (RMT)
- ERM Manager
- 

Department
- Business Units

Organizational Objectives
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
- Core internal audit roles
- Legitimate internal audit roles with safeguards
- Roles internal audit should not undertake

The Three Lines of Defense Model

Governing Body / Board / Audit Committee

Senior Management

1st Line of Defense
- Management Controls
- Internal Control Measures

2nd Line of Defense
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense
- Internal Audit

Adapted from ECIIA/FEFMA Guidance on the 8th EU Company Law Directive, article 41
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
- 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](http://www.cfo.gov)

AFERM: [www.aferm.org](http://www.aferm.org)

AGA: [www.agacgfm.org/resources/intergov/ermhub](http://www.agacgfm.org/resources/intergov/ermhub)