ENTERPRISE RISK MANAGEMENT (ERM) WORKING GROUP

MISSION

To contribute to the promotion and implementation of ERM principles in accordance with OMB Circular A-123 within the Offices of the Inspectors General (OIG) community.

SUB-GROUPS

- IMPLEMENTING AN ERM RISK ASSESSMENT APPROACH FOR AUDIT PLANNING PURPOSES
- AUDITING ERM IMPLEMENTATION AT COMPONENT AGENCIES
- ERM AT SMALL OIGS
- DEVELOPMENT OF AN ERM PRACTITIONERS’ GUIDE
“ERM as a discipline deals with identifying, assessing, and managing risks. Through adequate risk management, agencies can concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events.”

"(COSO) recognizes the increasing importance of the connection between strategy and entity performance..."  "Risk influences and aligns strategy and performance across all departments and functions."


The IG should provide for an assessment of the risks the OIG faces from both external and internal sources. Risk assessment includes identifying and analyzing relevant risks associated with achieving the OIG’s objectives, such as those defined in strategic and annual performance plans, and forming a basis for determining how risks should be managed.

2011
• Public Law 111-352, “GPRA Modernization Act of 2010”

2012
• CIGIE Quality Standards for Federal Offices of Inspector General, (“Silver Book”)

2014
• GAO Standards for Internal Control in the Federal Government (“Green Book”)

2015
• GAO-15-593SP, “A Framework for Managing Fraud Risks in Federal Programs”

2016
• Public Law 114-186, “Fraud Reduction and Data Analytics Act of 2015”

2016
• OMB Circular A-123, “Management’s Responsibility for Enterprise Risk Management and Internal Control”

2018*
• OMB Circular A-11, Part 6, “Strategic Plans, Annual Performance Plans, Performance Reviews, and Annual Program Performance Reports”

*Note: OMB Circular A-11 is subject to yearly updates
OIG’s Internal Role
OIG’S INTERNAL ROLE: TURNING ERM CONCEPTS INTO ACTION

1. Make the case for ERM
2. Build an ERM framework
3. Implement ERM
4. Integrate ERM, strategy and performance activities
5. Sustain ERM

Continuous communication with OIG leaders and staff

- Green: Completed
- Yellow: In progress
- Red: Future Action
OIG’S INTERNAL RISKS

Risk is the possibility that events may occur and affect the achievement of a business objective*

EXAMPLES

• Critical audits or investigations stopped due to a government shutdown
• Negative publicity regarding the OIG’s work could lead to a loss of reputation or credibility
• Lack of integrity in agency databases or records leading to inaccurate audit or investigation findings
• Outdated policies could create a culture of noncompliance or unaccountability among OIG employees
• Congress may have expectations that may exceed the OIG’s capacity
• Not leveraging data analytics in the risk identification process could diminish the impact of audits or investigations
• Talent pool may not be able to absorb departures

* Source: Committee of Sponsoring Organizations (COSO), Enterprise Risk Management – Integrating Strategy and Performance (June 2017).
WHY IMPLEMENT ERM?

• Ignored risks can become issues, which could become a crisis
• When risks are managed:
  • Respond quicker
  • With fewer resources
  • More options
• Improves the culture of the organization
• It is required
Risk Assessment

The COSO Framework defines risk assessment as “a process to identify, assess, respond to, and report on opportunities and threats that affect the achievement of objectives.”
What are the objectives/benefits of a Risk Assessment?

- Identify and assess risks in programs and processes that could impact operations and are mission critical to the Agency.

- Establish a formal risk-based engagement planning (e.g. annual work plan)

- Align OIG resources to areas that will provide the most value to the Agency.
Risk Assessment Process

1. Identify Audit Universe (audit segments)
2. Determine Risk Factors/Risk Criteria
3. Identify Risk Inventory/Risk Register
4. Rate Risks of each auditable segment (brainstorming session)
5. Calculate/assign overall risk score
6. Utilize risk assessment to develop annual work plan
OIG’S EXTERNAL ROLE: POTENTIAL RISK SOURCES*

Internally Identified Risks
- Strategic Planning and Priorities
- Program Performance, FEVS
- Internal Controls, Compliance
- Existing Risk Registers

Externally Identified Risks
- OIG Reports and Investigations (AGENCY)
- GAO Reports
- Laws and Regulations
- Congressional inquiries
- Customers/Stakeholders
- External reports (Media, Academic, NGO)

Emerging Risks
- External Operating Environment
- Forecasted Risk Issues, Projection Models
- Environmental Changes (Social, Economic, Environmental, Market/Industry, Political)

Agency ERM Risk Inventory

* For discussion purposes only. This illustration is not all-inclusive as Agencies have the flexibility to develop ERM approaches tailored to their organizations and responsive to Office of Management and Budget’s Circular A-123 requirements.
1. Risk Assessment of Programs
2. Evaluation of Agency Risk Management
3. Audit Reports and Recommendations to Agency
4. Investigative Work

**OIG**

**OIG Reports & Investigations**

- Information and Communication
- Responses and Requests

**Agency Management**

1. Risk Assessments
2. Control Activities
3. Implementation
4. Continuous Monitoring

Shared Goal: Improve Agency Programs and Operations
Objective: Identify criteria, share best practices, and develop guidance for OIGs seeking to assess (either audit or evaluate) agency ERM programs.

Deliverable: Draft Inspectors General Guide to Assessing Enterprise Risk Management, which:

- Describes OMB Circular No. A-123, the COSO ERM Integrated Framework, GAO’s Green Book, GAO’s Framework for Managing Fraud Risks in Federal Programs, the ERM Playbook, and relevant ISO and IIA documents.
- Summarizes various ERM reviews completed by GAO and OIGs since 2016.
- Presents steps OIGs may consider when assessing agency ERM programs, depending on objectives and scope of planned engagements.
- Includes ERM-related training resources that were available as of August 2019.
• Placeholder
OIG’S INTERNAL ROLE: TURNING ERM CONCEPTS INTO ACTION

1. Make the case for ERM
2. Build an ERM framework
3. Implement ERM
4. Integrate ERM, strategy and performance activities
5. Sustain ERM

Continuous communication with OIG leaders and staff