Collaborative Integration of Internal Controls, Enterprise Risk Management and Quality Assurance

Presentation to the QAWG
August 30, 2022

Dr. Temika Edwards, CIGIE ERM Co-Chair
OVERVIEW

- Enterprise Risk Management (ERM)
- Initiating ERM and Internal Control (IC) Integration
- ERM-IC Integration Framework
- How it All Comes Together
- Continuous Improvement
- Questions
**EVOLUTION OF ERM REQUIREMENTS**

- **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**

- **2016**
  - Public Law 114-186, "Fraud Reduction and Data Analytics Act of 2015"

- **2016**

- **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*
ERM AUTHORITIES AND GUIDELINES

OMB Circular No. A123


CIGIE Quality Standards for Federal Offices of Inspector General (Silver Book 2012), Section IV. D. Risk Assessments
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 ERM Process Framework provides a logical and systematic method for establishing the context for risks, as well as identifying, analyzing, evaluating, responding to, monitoring and communicating them in a way that will allow organizations to make decisions and respond in a timely manner to risks and opportunities as they arise.
THE VALUE OF ERM

• Ignored risks can become issues, which could become a crisis

• When risks are managed:
  • Respond quicker
  • With fewer resources
  • More options to meet the mission

• Improves the culture of the organization

• Enables a high performing organization

• It helps maintain a strong reputation
OIG’S INTERNAL RISKS

**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 could lead 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

---

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

* Source: Committee of Sponsoring Organizations (COSO), Enterprise Risk Management – Integrating Strategy and Performance (June 2017).
“(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.”

COSO’s Enterprise Risk Management
Aligning Risk with Strategy and Performance (2017)

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.

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:
- Integrating ERM principles to support agile **oversight**
- Assessing ERM implementation at component agencies
- ERM at **small OIGs**
- Development of an ERM Practitioner’s Guide (completed)
NEW! CIGIE Inspectors General Guide to Assessing Enterprise Risk Management

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 (IG) community.

Goals:

- Provide a forum for risk management professionals to share implementation challenges, solicit IG community input, and improve interagency communications.
- Disseminate the latest developments in ERM via expert guest lecturers.
- Develop a knowledge sharing platform and encourage exchange of leading practices.
- Maintain a specialized cadre of professionals to assist CIGIE Committees and/or member agencies in ERM related matters, via reimbursable agreement or detail.
- Coordinate with other professional ERM groups such as AFRM.

Related Pages

- Governing Documents
  - IG Act
  - Mission
  - Charter
  - Strategic Plan
  - Performance Plan

Committees

- Audit
  - Audit Peer Review

Budget

Technology

Inspection & Evaluation

Integrity

Investigations

Legislation

Professional Development

Workgroups & Roundtables

- Disaster Assistance Working Group
- Enterprise Risk Management (ERM) Working Group
- Federal Audit Executive Council

Sub-Groups

Quarterly Newsletters

ERM Resources

ERM Links
CIGIE ERM Working Group’s Practitioners Guide issued on October 2019

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
Objectives/benefits of a Risk Assessment:

• Uses an agile approach to work planning to effectively and efficiently respond to emerging issues.

• Identifies and assesses risks in programs and processes that could impact operations and are mission critical to the Agency.

• Establishes a formal risk-based and data driven engagement planning (e.g. annual work plan).

• Aligns OIG resources to areas that will provide the most value to the Agency.
OIG’S EXTERNAL ROLE: POTENTIAL RISK SOURCES*

**Internally Identified Risks**
- Strategic Planning and Priorities
- Program Performance, FEVS
- Internal Controls, Compliance
- OMB ERM maturity model (gaps and opportunities)

**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)

*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.
RELATIONSHIP BETWEEN ERM & INTERNAL CONTROLS

ERM & Internal Controls

Three Lines of Defense

Governance
Enterprise Risk Management
Risk Management
Internal Controls

Senior Management

1st Line of Defense

Financial Control
Security
Risk Management
Quality
Inspection
Compliance

2nd Line of Defense

3rd Line of Defense

Internal Audit/Quality Assurance

Governing Body/Risk Mgmt Council

External Audit
Regulator
RELATIONSHIP BETWEEN ERM & INTERNAL CONTROLS
CUBE VERSION

A-123 Sec2on III. Update
(Internal Controls)

A-123 Sec2on II. Update
(Enterprise Risk Management)

Source: Based on COSO
Source: GAO Green Book
Integration in Advanced Maturity Stages

Integration of ERM and Internal Controls typically is possible at an advanced stage of maturity.
- Leverage existing IC capabilities
- Build ERM capabilities
- Partner throughout the process
KEY STEPS IN INITIATING ERM-IC INTEGRATION

- Initiate communication across the ERM and IC functions
- Document the ERM and IC activities that are already occurring or are planned for your organization
- If applicable, develop separate ERM and IC Charters that communicate the authorities and scope of ERM and IC activities as well as roles and responsibilities
- Consider the categories of risk where integration might be more intuitive, e.g. operational risks, resource management
- Create mechanisms for discussion of internal controls at an agency level, e.g. governance structure, integration of risk into existing management committees
ERM AND QUALITY ASSURANCE – MAINTAINING INDEPENDENCE

Figure 2
The Role of Internal Audit in ERM

Source: The Institute of Internal Auditors, Inc. and the Risk and Insurance Management Society, Inc.
INITIATING ERM-IC INTEGRATION – LESSONS LEARNED

- Must integrate – not optional
- Integration does not mean combining functions into a single organization, unless preferred
- ERM and IC leaders should speak frequently and informally
- Make sure ERM and IC personnel understand their shared terminology and can explain it effectively to others
- Understand where to draw the lines between functions
- Be patient – integration of ERM-IC at your organization is NEW, no one has all the answers.
# Tips to Avoid Pitfalls When Preparing to Implement ERM & Integrate Internal Controls

## ERM not Integrated
ERM should not be an isolated exercise, but instead, should be integrated into the management of the organization and eventually into its culture.

## Failing to Work Closely with Business Leaders
The ERM program’s first questions to agency managers should always be: What are your major risks? And how can we better support you in better managing them? Collaborations should occur early on in the implementation and integration efforts.

## Absence of Support from Senior Leaders
Strong leadership at the top of the organization (active participation and oversight) and participation/engagement from business line leaders is critical.

## Too Much too Quickly
The top two or three risks or a type of risk. ERM is an iterative effort that develops over time. Management may consider an incremental approach, initially focusing on the top two or three risks or a type of risk.

## Focusing too much on Internal controls
ERM includes internal controls but also larger issues of the external environment, as well as transparency, business practices, reporting, and governance that help define the overall risk culture.

## Reinventing the Wheel
Don’t reinvent the wheel. Instead, organizations should customize their approach to fit their unique environments. There is no cookie-cutter approach ERM and Internal Controls integration.
Does your agency have a framework for integration of ERM and internal control?

a. Yes
b. No
The Framework represents over a year of open discussion between ERM-IC leadership and followed numerous joint ERM-IC engagements and training events.

Don’t try to force a framework – adopt what works from other models and adapt to your own organization as needed.

Both ERM and IC are equally important

Identify ways to leverage existing ERM and IC activities to run-through ERM-IC integration so that it happens organically

Start in areas where you already have established expertise or support
Are you actively working to integrate ERM and internal control?

a. Yes  
b. No
Tailor your model to your organization. Balance formal with informal mechanisms.

Identify communication gaps and be open to unique solutions.

Any new governance model requires training for participants and messaging on value proposition (benefits outweigh the investment).

Start small; remain focused on “comfort zone” or “hot topic” areas. Expand the scope as the organization grows and matures.

Risk management occurs at all levels of the organization, but individuals must do so purposefully and with a clear understanding of why.

Develop tools and practical examples to educate others on how to apply your framework.
Integrated Approach to Enterprise Risk Management

The ERM framework manages risks to the organization’s internal processes, people, systems and external events. These activities provide the organization with actionable, meaningful outcomes for leadership.
INVITE AN EXPERT TO CHALLENGE PLAN QUALITY

ERM and Internal Audit Partner to Challenge Risk Owners’ Plans

Illustrative Example

Can you share some details on how you incorporated the XYZ findings from the last audit report in your risk response plan?

After this issue was raised in the last audit report, we’ve restricted XYZ to individuals and teams handling non-sensitive data assets.

ERM’s Contribution
- Ensuring a consistent methodology for assessing risks and response efforts
- Sharing examples of how different groups in the organization are addressing similar problems

Internal Auditors validate and verify the self-assessments and response plans
• Continue to mature ERM within the OIG community

• Integrate ERM with strategy and performance.

• Implement Quality Assurance Review recommendations:
  o Describe communication plan for Risk Profile update
  o Distinguish Risk Register from Risk Profile
  o Link Risk Profile to ERM Action Plan