Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

Enterprise Risk Management Practitioner's Guide for Offices of Inspectors General

OCTOBER 2019

EXECUTIVE SUMMARY

Purpose

The purpose of the *Enterprise Risk Management (ERM) Practitioner's Guide* is to provide good practices and share lessons learned to Federal Offices of Inspector General (OIG) that seek to develop and implement an ERM program. This guide offers practitioners insights and considerations on how to identify and manage potential risk events that may affect mission goals and objectives, as well as a how to develop a basic governance and management structure to oversee and implement risk management activities. The guide facilitates implementation of the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Silver Book, the Office of Management and Budget (OMB) Circular A-123, the *Fraud Reduction and Data Analytics Act of 2015*, and other applicable guidelines.

Approach

Members from ten OIG organizations with expertise in ERM volunteered to share their good practices. They participated in workshops and group discussions leading to the development of this guide. The guide was subject to extensive review to ensure harmonization, readability, and plain language.

As with all public sector organizations, OIGs face risks to achieving their mission, goals, and objectives. Risks associated with talent recruitment and retention, complex operations, technological breakthroughs, public perception, budget shortfalls, and organizational culture may not promote OIG engagement, high performance, or transparency.

OIGs need to identify risk challenges that lie ahead to remain flexible, respond to changes in their particular risk environment, and create public value. ERM is a useful process that improves decision-making by providing an understanding of both risks and opportunities associated with mission accomplishment. Essentially, ERM is a holistic approach that uses an enterprise-wide lens to identify and prioritize internal and external risks to the organization, along with related mitigation efforts. The key to an effective ERM capability is for entities to understand the combined impact of risks in an interrelated portfolio, rather than by addressing risks only within silos.

The objective of this guide is to share good practices for ERM implementation activities in an effort to facilitate the adoption of ERM within the OIG community. This guide is not prescriptive. Each OIG should take into account the strength of its existing risk management controls, budget, organizational culture, and structure and size before choosing to develop an ERM implementation strategy. That is, each OIG should customize an ERM approach that complements its unique mission, vision, core values, goals, objectives, and available resources. Although the good practices described in the guide highlight the experiences of practitioners within the IG community, these experiences can serve as a useful resource for any Federal agency or public sector organization seeking to implement or enhance ERM practices.

The contributors to this guide, a group of ERM professionals within OIG organizations, have had the opportunity to plan, champion, and implement ERM programs within their organizations, while experimenting with different approaches and techniques along the way. During the development of this guide, working group members relied on their expertise, combined with real-world experiences, to steer the reader through developing, implementing, integrating, and sustaining ERM.

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

INTRODUCTION 1

Background 1

CIGIE Enterprise Risk Management Working Group 1

How to Use This Guide 1

ERM CONSIDERATIONS 3

Seeking ERM Champions 3

Placement of the ERM Function 5

Reporting Lines 5

ERM Staffing 6

Risk Management Council 7

Organizational Culture 8

Available Guidance 9

DEVELOPING AN ERM FRAMEWORK 11

Implementation Plan 12

Strategy and Objectives 12

Establishing the Context 14

Internal Considerations 14

External Considerations 14

Developing Risk Categories 15

Risk Attitude 16

Risk Management Philosophy 16

Risk Appetite 17

Risk Tolerance. 19

Risk Assessment 19
Risk Rating Criteria 19
Risk Assessment Scales 20
Impact Rating Criteria 20
Likelihood Rating Criteria 20
Effectiveness of Controls Rating Criteria 22
Risk Velocity Rating Criteria 22
Scoring and Depicting Results 23
IMPLEMENTING ERM 26
Leveraging CIGIE, Federal Agencies (non-OIG), and Private Sector Networks 26
Record Keeping of Enterprise Risk Management Materials 27
Risk Management Discussions with Your Agency 27
Identifying Risks 28
Planning In-Person Interviews 29
Conducting Interviews 30
Aggregating and Analyzing Risks 31
Inherent Risk and Residual Risk 32
Developing a Risk Profile 32
Approaches for Developing a Risk Profile 33
Analyzing Risks 34
Implementing Risk Appetite 35
Leveraging the Risk Profile to Enhance Internal Controls and Decision-Making 36
Visualization Options 37
Leveraging Other Data Sources 37
Responding to Risk 38

Developing Risk Mitigation Plans and Progress Monitoring 39
Monitoring Risk 39
Assessing Risk 40
INTEGRATING AND EMBEDDING ERM WITHIN ORGANIZATIONAL CULTURE AND OTHER PROCESSES 41
Fraud Risk 41
Fraud Risk Factors 41
GAO Framework for Managing Fraud Risks 42
OMB's Perspective on Fraud 42
Leveraging Disparate Processes to Integrate Fraud Risk 43
General Interviews and Entity-Level Risk Assessments 43
Leveraging Quality Assurance Reviews 44
Leveraging Internal Affairs Investigations 45
Leveraging Strategic Planning 45
Leveraging Performance Management 47
SUSTAINING ERM 50
Building Capabilities 50
Training 51
Subscription Service and Outside Vendors 51
Crowdsourcing 51
Automation Resources 52
Maturity Model 52
Identifying and Improving Risk Culture 53
EXHIBIT A: APPLICABLE LAWS AND POLICIES 55
EXHIBIT B: RIMS™ ERM MATURITY LEVELS 66
EXHIBIT C: STRATEGIC PLAN EXAMPLES 67

EXHIBIT D: RISK CATEGORIES, DEFINITIONS, AND EXAMPLES 73

EXHIBIT E: OTHER RISKS TO CONSIDER 76

EXHIBIT F: GLOSSARY 78

EXHIBIT G: REFERENCES 83

EXHIBIT H: LIST OF PARTICIPATING OFFICES OF INSPECTOR GENERAL 85

INTRODUCTION

Background

The Committee of Sponsoring Organizations (COSO) defines Enterprise Risk Management (ERM) as a process applied in strategy settings across an entity, designed to identify potential events that may affect the organization and to manage risks within the organization's risk appetite[1] to provide assurance regarding the achievement of entity objectives.

The underlying premise of ERM is that all organizations exist to provide value for their stakeholders. All organizations face uncertainty, or risk, and the challenge for management is to determine how much risk to accept as the organization strives to provide value. Federal managers must carefully consider the appropriate balance between risks, controls, costs, and benefits in their mission-support operations. Too many controls can result in inefficiencies, while too few controls might increase risk to an unacceptable level.

CIGIE Enterprise Risk Management Working Group

The Council of Inspectors General on Integrity and Efficiency (CIGIE) established an ERM working group, composed of representatives from various organizations, to contribute to the promotion and implementation of ERM principles in accordance with Office of Management and Budget (OMB) Circular A-123 within the Offices of Inspector General (OIG) community. ERM working group efforts directly support CIGIE's mission to identify and address issues that transcend individual Government agencies and enhance the professional development of the OIG workforce. The ERM working group is open to all interested Federal personnel assigned to matters related to implementation, oversight, or auditing of ERM programs. Participating agencies include any of the statutory OIGs.

As part of this effort, the ERM working group assembled in several subgroups to address multifaceted topics regarding ERM and the OIG community, including a subgroup responsible for developing guidance on how to implement ERM within an OIG organization.

How to Use This Guide

This *ERM Practitioners' Guide* (guide) represents a collaborative effort undertaken by several OIG staff members committed to the advancement of ERM. To help develop this guide, ten participants volunteered their insights and experiences in planning and implementing ERM within their respective OIG organizations.

The objective of this guide is to share good practices for ERM implementation activities to facilitate the adoption of ERM throughout the OIG community. However, this guide is not prescriptive as each organization should take into account its unique mission, vision, core values,

[1] See "Developing an OIG ERM Framework" for a complete discussion of "risk appetite."

goals, and objectives. In addition, this guide should not be considered a mandate to implement ERM, or provide the basis for a peer review within the OIG community. OIG organizations have the unique flexibility to choose to establish an ERM program voluntarily, as they deem appropriate[2].

This guide does not address ERM implementation as a methodology to identify areas of audit investigation or other functional areas of oversight. It rather provides a comprehensive hands-on approach to organizations seeking to implement a formal ERM program internally to optimize mission accomplishment and create public value through proactive risk and opportunity management.

This guide offers practical insights on key ERM implementation topics such as: (a) ERM considerations, (b) developing an OIG ERM framework, (c) implementing ERM, (d) integrating and embedding ERM within organizational culture and other processes, and (e) sustaining ERM.

ERM will evolve over time as lessons learned and good practices are shared among Federal ERM practitioners. For the OIG community, we have the unique opportunity to leverage ERM to strengthen our reputation, as well as to emphasize trust, collaboration, improvement, and continuous learning and growth among all members of our staffs and our stakeholders.

[2]Some OIGs are not components of an entity legally defined as a "Federal agency." Therefore, some laws, regulations, or other guidance may not be directly applicable by law to all OIGs. In these cases, principles or concepts in the laws, regulations, or other guidance may be adopted by the OIG entities as a matter of policy.

ERM CONSIDERATIONS

As participants in the working group led ERM initiatives in their respective offices, they found themselves spending a lot of time championing the idea to leaders, managers, and staff. Crucial to implementing a successful ERM program is to develop and clearly communicate the value of ERM, including the expected benefits of implementation. That value must be supported by proper organizational placement and strong executive sponsorship, and it should fit into the existing overall culture and subcultures within the organization, along with available criteria and guidance.

Seeking ERM Champions

Participants said that ERM can fail to get started because of insufficient stakeholder support, resources, or understanding on how to implement the program. Seeking ERM champions and gaining organizational buy-in was an important first step.

For some participants, dealing with a large-scale issue or crisis helped propel an organizational interest in adopting ERM. Nonetheless, the need to describe the benefits of ERM implementation in terms of both individuals and the OIG as a whole cannot be underestimated. Participants noted the importance of focusing on characteristics inherent to the OIG culture and the role it plays in the Federal Government. Namely, OIGs continuously strive to lead by example and to protect the public trust.

While seeking championship, participants articulated how ERM can help build and maintain OIG's reputation of good stewardship and leadership in good management practices. Participants made the case that ERM could be leveraged to avoid reacting to risk events after they occur, which can ultimately erode public trust. Moreover, they emphasized that if OIG organizations are to hold agencies accountable for managing risk, they must also be accountable for managing risk; otherwise, they could lose credibility.

Participants highlighted the following value propositions when seeking champions and organizational buy-in for ERM:

- ERM advances governance through improved mission delivery, reduced costs, focused corrective actions, and increased transparency. ERM is a proven process to identify and manage risk, which can have a positive effect across the organization at the executive level (and beyond).

  Participants agreed that senior management plays an important role in governance and the adoption of ERM. The ultimate goal is to accelerate ERM leaders' effectiveness by defining key responsibilities. Often expectations and goals from stakeholders can conflict with one another, creating challenges for ERM staff. Without a cohesive focus on stakeholder expectations, the ERM program could be developed in an ad hoc, reactive manner.

- ERM can enhance organizational culture. Culture encompasses the organization's core values, beliefs, attitudes, and desired behaviors on the importance of understanding risk, which (collectively) may impact the achievement of its mission and vision.

  Risk management is not new to the OIG community; in fact, it is something we do every day. Implementation of ERM can heighten awareness about risks and risk management, enhance engagement and trust throughout the organization, and create a safe place for managers and employees to discuss concerns. In this way, ERM can enhance the culture of the organization overall, in terms of risk awareness, and increase the skill sets of employees in regard to how they think about and respond to risk. Potentially, benefits of a culture change can contribute to better decision-making and a more engaged workforce.

- ERM is rapidly being adopted by Federal agencies, including OIG organizations.

Within the OIG community, two organizations fully adopted ERM initially, namely, the Pension Benefit Guaranty Corporation and the U.S. Department of Labor. Notwithstanding the differences between these two organizations (staff size, mission, geographic footprint, and level of resources) and distinct approaches to ERM, both Inspectors General (IG) successfully championed and implemented ERM. The successful implementation efforts within their organizations demonstrated that ERM is not a "one size fits all" process, but rather a tailored process designed to meet the needs of the organization. Their experiences also demonstrate that ERM can be beneficial to organizations of all sizes.

The championing and support provided by these two IGs created momentum within the community, resulting in continued efforts to expand buy-in from leadership, management, and staff by reinforcing the value proposition for ERM. In particular, these OIG organizations adopted the following practices:

- communicated ERM benefits in writing, most often in the organization's ERM framework;

- developed and implemented a risk assessment process that included employee input as well as management perspective;

- ensured transparency, both in terms of the process and the results, sharing plans and results via email or posting that information to community web pages; and

- demonstrated that ERM had the full support of leadership by establishing a Risk Management Council (RMC) inclusive of top leadership, as well as identifying an ERM champion at the executive level.

Organizational Governance

Participants said that executive support, organizational placement, and staffing for ERM would indicate to managers and staff how important ERM is to the organization's leaders and should help establish a proper governance structure. Identifying an ERM champion, preferably at the executive

level, can help communicate the importance of ERM to other executives and to demonstrate that top leaders embrace the initiative. It is also important to place the ERM function within an office or division that has access to the organization's leaders and has the resources (or access to resources) to facilitate or execute ERM activities. Placing appropriate emphasis on ERM has the added benefit of changing perceptions within the organization. Maintaining buy-in among staff members, especially at the executive level, will further aid in conducting risk assessments, because it can help break down internal resistance to what can be seen as simply another level of bureaucracy.

Governance refers to the allocation of roles, authorities, and responsibilities among stakeholders, senior management, and field management components. The common steps to establish ERM for governance among the participants included: (1) placement of the ERM function; (2) determining reporting lines and staffing; and (3) establishing a separate RMC (or leveraging an existing senior-most governance forum), and chartering this function.

Placement of the ERM Function

Participants shared that their organizations undertook a range of approaches to establish an ERM function.[3] Participants' placement often allowed them to engage with senior leadership either on ERM implementation or on matters related to strategy development, performance management, and risk. To develop a more enterprise-wide perspective, participants also took part in senior leadership meetings relative to nearly all aspects of OIG business. Keep in mind that there is no "right" or "wrong" approach to determine placement of the ERM. Practitioners must consider an approach that provides the most opportunities for executive communication given their organizational culture, chain of command, and grade level. Other relevant factors include organizational size, budget, mission, geographic disbursement, and organizational structure. Having the ERM function clearly identified and defined within the organizational structure helps eliminate internal confusion about who is ultimately responsible for ERM.

The responsibilities of the ERM functions also varied among the participating OIGs. One example included forming a cross-functional internal group representing all levels of the OIG responsible for advancing the ERM framework. The cross functional group's responsibilities included: (a) creating tools, templates, and training modules; (b) issuing guidance; (c) conducting risk analyses; and (d) soliciting stakeholder feedback. Another participant established an internal group to assess the quality and maturity of the ERM function. The tasks involved evaluating the: (a) risk management processes; (b) management of key risks, including the effectiveness of implemented controls and any other control activities; and (c) appropriateness of the risk assessment process, including the reporting of risks and controls status.

Reporting Lines

Among participants, the ERM function is assigned to various offices or divisions with various reporting lines and staffing levels. Units responsible for managing ERM often have other collateral, generally related duties. These duties typically include areas such as strategic planning,

[3] See "Developing an OIG ERM Framework" for additional discussion.

performance management, and quality assurance. Placing ERM alongside these synergetic functions can assist with integration.

Titles among participants included ERM Directors, Chief Performance and Risk Management Officers, Assistant Inspectors General (AIG) for ERM, and others. Staff responsible for leading ERM efforts have different reporting lines within their organizations, including to the Chief of Staff (with a dotted line to the front office), to the IG, to a Deputy IG, or to a director of a division responsible for ERM and other missions. Participants agreed that the responsible ERM official should hold a direct reporting line to the IG or to a Deputy IG. Direct reporting is critical to ensure greater transparency, to ensure greater independence, and to raise the profile and focus of ERM capabilities. Moreover, open and candid conversations should become a natural part of the ERM landscape.

ERM Staffing

While almost all participants have some level of dedicated staff to support ERM efforts, such staff can be assigned other duties depending upon the portfolio of the office. In some instances, staff members are temporary (detailed employees or contractors). Participants generally reported at least one full-time equivalent (FTE) dedicated to ERM with staff size ranging from one to four FTEs. Volunteers from other OIG offices, especially for sensitive or confidential projects, were common in OIG ERM offices. The participants expected no future increases in ERM staff from current levels. Generally, OIGs do not have the overall capacity to support a large ERM staff.

Participants thought it was important to understand the skill sets, capabilities, strengths, and backgrounds of the ERM team. This understanding can help determine skill gaps and identify areas of growth and development among the team. For example, although auditors and accountants have a thorough understanding of internal controls, compliance, financial management, and risk assessment, they may not possess project management and enterprise-wide strategic planning skills. Similarly, strategic planners often have a holistic, prospective view of the organization and are familiar with program and project planning, but they may not have experience managing daily, tactical activities, or facilitating and assessing risk mitigation activities through risk owners. To be effective, ERM staff must understand the internal workings of the organization and have strong quantitative and interpersonal skills.

Skills and competencies that contribute to an effective ERM program are wide-ranging and include:

- **Soft skills:** Influence, diplomacy, empathy, relationship management, facilitation, customer service, and interpersonal communication.

- **Strategic thinking**: Business intelligence, reasoning, problem solving, objective definition and prioritization, and flexibility.

- **Functional knowledge:** ERM concepts and frameworks, risk management, cross-functional knowledge (HR, procurement, IT, budget, etc.), organizational knowledge, and mission operations knowledge.

- **Technical skills**: Data analysis and visualization, root-cause analysis.
- **Process management:** Project management, process improvement, and change management.

Risk Management Council

The purpose of the RMC is to incorporate ERM concepts into the strategic decision-making process so that an organization can effectively achieve its mission, vision, and objectives. The RMC should strongly support and commit to the OIG's core values and enforce transparency and accountability by clearly communicating expectations for managing risks and establishing ERM practices and capabilities. OMB A-123 identifies a similar body as the Senior Management Council. Therefore, organizations should consider leveraging existing governance bodies for the purposes of ERM.

For example, the RMC should:

- set the "tone at the top" in support of the ERM process;
- encourage staff to elevate risks and critical issues in a timely fashion;
- enable risk-informed decision-making and eliminate barriers to promote such activity;
- establish the risk appetite and tolerances;
- identify high-priority existing and emerging risks;
- decide how to respond to identified risks in concert with risk owners;
- ensure identified risks are reported, analyzed, monitored, and tracked;
- support implementation of effective mitigating strategies and controls;
- assess organizational performance; and
- establish the organization's risk profile[4] within the established risk tolerance thresholds, risk appetite, and other related policies.

Participants reported that the ERM function or internal group is part of, or at least collaborates with, a larger collection of representatives of offices within their respective organizations. Some participants' efforts are more advanced than those of others in this regard. For example, the enterprise-wide group mentioned previously presents its proposed annual plan and means of execution to their RMC, composed of senior staff. For another participant, the ERM program is part of a Quality Assurance and Standards Directorate, which assigns ERM responsibilities to the

[4] See "Implementing ERM" for a discussion of "risk profile" for additional discussion.

Chief of Staff, an RMC, and a Risk Management Working Group. Although ERM functions are in various states of maturity, all of them report working with an RMC to some extent. The existence of an RMC is a good practice encouraged by OMB Circular A-123.

The roles and responsibilities of most RMCs should be set forth in a charter. A charter is extremely useful in establishing expectations for all participants up front and should be updated based on the evolving needs of the RMC. Based on participants, an RMC generally includes the IG, Deputy Inspector General (DIG), legal counsel, AIGs, and other senior management. The RMC may also include the Chief Risk Officer (CRO), a Chief Performance and Risk Management Officer, or the individual responsible for heading up ERM activities and the internal working group. For one participant, the RMC also included the Ombudsman, Equal Employment Opportunity (EEO) manager, and the Employee Advisory Council (by invitation only). Nonetheless, for the composition of the RMC, senior leadership inclusiveness is extremely important to facilitate transparency and buy-in.

Organizational Culture

An organization's culture reflects its core values, behaviors, and decisions. Management decisions are, in turn, a function of the available information, judgment, capabilities, and experience. An entity's culture influences how the organization applies its ERM framework, how it identifies risk, what types of risk it accepts, and how it manages risk (COSO 2017).

> An entity with a culture that is risk-aware stresses the importance of managing risk and encourages transparent and timely flow of information. It does this with no assignment of blame, but with an attitude of understanding, accountability, and continual improvement (COSO 2017).

Table 1 illustrates some of the core values of the participants' organizations. Although no single participant included all of the listed core values in its ERM framework, each core value certainly applies. Organizations must tailor their ERM framework to fit their unique structure and cultural attributes. Failing to do so increases the likelihood that the ERM initiative will not be fully embraced or effective throughout the organization.

Table 1: Example of OIG Values Included in ERM Frameworks

Core Values	
Accountability	Taking ownership of our decisions and actions. We hold one another accountable to a higher standard of conduct.
Courage	Doing what is right, no matter how difficult. We ask questions and raise concerns when needed.
Excellence	Delivering relevant, quality, timely, high-impact products and services, through a workforce committed to accountability and the highest professional standards.

Core Values	
Independence	Committing to being free of conflicts of interest through objectivity and impartiality.
Integrity	Adhering to the highest ethical principles and performing our work in an honest and trustworthy manner.
Respect	Appreciating the uniqueness of our workforce. We treat others with dignity, civility, and mutual consideration.
Service	Demonstrating the vigilance to duty through dedicated public service as a unified team.
Stewardship	Accepting our responsibility to serve the public good. We care about leaving things better than we found them.
Transparency	Promoting an environment of open communication through information sharing, accountability, and accurate reporting.
Trust	Keeping promises, delivering on commitments, and communicating honestly with our stakeholders.

The way values are communicated across the entity is referred to as the tone of the organization.

> A consistent tone establishes a common understanding of the core values, business drivers, and desired behavior of personnel. The more the tone can remain consistent throughout the entity, the more consistent the performance of enterprise risk management responsibilities in pursuit of the entity's strategies and objectives will be (COSO 2017).

The characteristics needed to achieve the desired culture over time include maintaining strong leadership, employing a participative management style, enforcing accountability for all actions, aligning risk-aware behaviors and decision-making with performance, embedding risk in decision-making, having open and honest discussion about risks facing the organization, and encouraging risk awareness across the entity.[5]

Available Guidance

In August 2012, the CIGIE issued the *Quality Standards for Federal Offices of Inspector General* (Silver Book[6]), which established a quality framework for managing, operating, and conducting the work of OIGs. The Silver Book provides guidance regarding risk management within OIG organizations, including "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."

[5] See "Identifying and Improving Risk Culture" for additional discussion.
[6] https://www.ignet.gov/sites/default/files/files/Silver%20Book%20Revision%20-%208-20-12r.pdf

In July 2016, the Office of Management and Budget revised Circular No. A-123, *Management's Responsibility for Enterprise Risk Management (ERM) and Internal Control* (Circular). The revised Circular reinforced the purpose of the *Federal Managers' Financial Integrity Act* (FMFIA) and the *Government Performance and Results Act Modernization Act* (GPRAMA[7]). It required agencies to implement an ERM capability coordinated with the strategic planning process as well as the internal control processes as established by FMFIA, GPRAMA, and the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book[8]).

It is important for ERM practitioners to stay abreast of the latest developments regarding ERM good practices, as well as oversight reports developed by the Administration, Congress, or GAO. Staying abreast may be accomplished through related news articles, exchanges of information with other ERM practitioners, and other networking venues.

[7] Available guidance, applicable laws, and summaries of what they say about ERM are at Exhibit A of this guide.
[8] https://www.gao.gov/greenbook/overview

DEVELOPING AN ERM FRAMEWORK

Participants agreed that integrating ERM throughout an organization is most effectively done when a framework is developed first. A framework is a key first step that can define the aspects of a formal ERM program and lead to improved decision-making in governance, strategy, objective setting, and day-to-day operations. Developing an ERM framework should not be underestimated because it sets a foundation and creates the diligence required to integrate ERM within an organization. An ERM framework sets a clear path to creating, preserving, and realizing value (COSO 2017).

The three essential elements for developing a successful ERM framework include:

- developing a common risk language so that all employees speak the same language when discussing and managing risks to ensure effective and quick communication across the organization;
- developing an effective organizational structure that promotes the early identification, assessment, and management of key risks; and
- creating a process that embeds risk management within all key processes to ensure that risks can be managed effectively (*Auditor's Risk Management Guide*).

Regardless of how an organization chooses to approach ERM, a structured approach set forth in an ERM framework will help with the implementation and operation of ERM. Agencies may choose to adopt particular standards or frameworks (COSO, ISO 31000), but, whichever framework an agency selects, it is important that the agency customizes it to meet the mission, needs, structure, and culture of the organization (*Performance Improvement Council Playbook*). The primary focus for customizing an OIG ERM framework requires:

- recognizing organizational governance, including organizational structure, roles, and responsibilities;[9]
- recognizing organizational culture;[10]
- developing an implementation plan;
- establishing a strategy and objectives;
- articulating risk attitude; and
- developing risk evaluation criteria.

[9] See "Organizational Governance" for additional discussion.
[10] See "Organizational Structure" for additional discussion.

Participants emphasized that the ERM framework should not be a static document. Rather, the framework should be a living document, reviewed, edited, and expanded regularly as ERM matures. Moreover, the framework should be principled and not prescriptive, because it is important to allow managers and staff room for implementation.

As part of the framework development, it is also important to establish a 1- and 3-year strategy for implementing and maturing the ERM function. Understanding the vision for the program and outlining tactical implementation steps over a single and multiyear horizon helped participants communicate priorities with senior management and staff.

Implementation Plan

In addition to the ERM framework, participants have developed a project implementation plan (IP), or some other written mechanism to outline and document the ERM implementation process and milestones. The IP should be in sufficient detail (yet not overly complex) with a clear description of each implementation step, targeted milestone dates, and a listing of the responsible position(s) for each implementation step. Further, participants recommend developing the IP in collaboration with stakeholders. In this way, the practitioner may tailor the IP to resolve ERM conflict and other key organizational activities and deliverables (e.g., publication of the Semi-Annual Report, Top Management Challenges, etc.), as well as to consider the strengths and expertise of each individual office or team member, as applicable.

Strategy and Objectives

Participants agree that an important factor in implementing an effective ERM framework and process is to first have a strategy that defines the activities an organization will undertake to achieve its mission and vision. According to the CIGIE Silver Book, "each OIG shall maintain a planning system assessing the nature, scope, and inherent risks of agency programs and operations. This assessment forms the basis for establishing strategic and performance plans, including goals, objectives…to be accomplished by the OIG within a specific time period." This guidance affirms the fact that it is essential for OIG organizations to have clear strategic goals and objectives to demonstrate public value regardless of ERM activities.

While most OIG organizations have strategic plans in place, such plans should include well-defined strategies that drive the efficient allocation of resources and effective decision-making. A strategic plan should also include objectives that serve as a roadmap throughout the organization's units, divisions, and functions. According to best practices, when developing a strategic plan the organization should consider the external and internal environments and stakeholders. Involvement from all OIG component offices should be viewed as a necessity, not an option.

Participants viewed the external environment as generally including political, economic, social, technological, legal, and environmental factors. The internal environment often includes capital, people, processes, and technological factors.

Objectives help to establish a common understanding among internal and external parties regarding what the organization is trying to achieve, its operating philosophies, and expected standards of conduct. The key is to develop objectives that are specific, measurable or observable, attainable, and relevant. Equally important is articulating the barriers to success and uncertainties, which represent the risks facing an organization. Failing to anticipate and understand these risks can make achieving the objectives much more difficult. Specifically, objectives that do not align or only partially align with the strategy may introduce unnecessary risk. That is, the organization may use resources that would be more effectively deployed in carrying out other objectives. Simply put, the ERM programs used by the participants so far will primarily explore the risks and opportunities associated with an OIG's strategic goals and objectives.

The OIG community has its mission rooted in its statutory responsibilities under the IG Act. The CIGIE Silver Book, GPRAMA, and OMB Circular A-11, Part 6, provide substantial guidance for developing a strategy and expressing performance management. Other considerations when developing an OIG strategy are the Department's mission, strategic plan, management challenges, and major program development and initiatives. Table 2 summarizes examples provided by participants.

Table 2: Examples of OIG ERM Strategies

Mission	Vision	Objectives/Goals
Promote the economy, efficiency, and effectiveness of agency programs and operations. Protect the integrity of agency programs and operations.	Committed to excellence, innovation, core values, and sharing knowledge and best practices. Heighten awareness of agency's toughest challenges and support agency's efforts to meet its mission.	Further the agency's mission success. Advance operational economy, efficiency, and effectiveness. Cultivate positive internal and external stakeholder relations. Invest in organizational culture and ourselves. Foster strategic thinking and long-term planning.
Provide independent and objective oversight.	Enhance agency's ability to address emerging workforce challenges. Foster a thriving work environment that values employees.	Deliver timely, relevant, and high-impact results. Foster an internal OIG culture that drives high performance and engagement. Promote responsible stewardship of OIG financial and non-financial resources.

An OIG organization should expect that the strategy it selects could be carried out within its risk appetite; that is, strategy must align with risk appetite. The participants noted that, if the risks associated with a specific strategy are inconsistent with the organization's risk appetite, they need to be revised, an alternative strategy selected, or the risk appetite revisited.

Establishing the Context

Participants shared that the initial step in developing an ERM framework is to establish the context, which means understanding and articulating the internal and external environments of the organization. Participants said that this step required them to be innovative including soliciting contextual input from stakeholders, understanding relevant laws and mandates (related to the OIG environment), and gaining familiarity with OIG's unique mission, objectives, and organizational culture. It is also important to have a solid understanding of the external environment, including societal dynamics and changes.

Internal Considerations

Participants considered the unique laws and responsibilities that are crucial in shaping the internal environment and mission of an OIG. For example, the *Inspector General Act of 1978* was established in response to a series of government scandals, establishing IGs across government agencies, and charging them with a unique responsibility. Because of the IG Act, objectivity, integrity, transparency, and independence became key values and drivers of mission operations and IG culture that must be understood and considered.

OIG senior leadership must also play a critical role in the process of developing and implementing an ERM Framework. Understanding internal dynamics, leadership style, organizational structure, and culture is pivotal to developing an actionable framework. The OIG executive team often assists participants by sharing environmental conditions, determining an actionable focus, and identifying any regulatory or fiscal barriers, which could affect the ERM implementation process.

External Considerations

Participants understood that they needed to consider key external dynamics and societal trends (e.g., technology, public perception of government, demographics). They kept abreast of world and national news by reviewing research work conducted by outside entities such as the Pew Research Center,[11] Project on Government Oversight,[12] The Urban Institute,[13] and other bodies of respected, unbiased experts that provide research, advice, and ideas on specific political, societal, or economic problems.

[11] http://www.pewresearch.org/
[12] https://www.pogo.org/
[13] https://www.urban.org/

Participants also considered relationships with Congress and the agencies affected by OIG work. To account for legislative and fiscal trends, they collaborated with OIG staff members with expertise in Congressional and public relations and legal and financial management.

Developing Risk Categories

It is common for a risk assessment to identify several risks. Moreover, when conducting risk assessments, it is important to consider the risk of fraud. Participants agreed that creating a risk model that groups risks into categories based on the nature of the risks provides a structure to make it easier to understand the results. Risk categories typically have broad risk areas (e.g., strategic, environmental, operational, financial, informational) and groups within the risk areas to further categorize the risks. Risk categories may look like the following (Sobel 2015):

- **Strategic Risks:** Risks that impact the nature and viability of the organization's business model:
  - **Internal risks** are caused by, sourced from within, or manageable from within the organization.
  - **External risks** come from outside the organization.

- **Operational Risks:** Risks that impact the effective operation of the business:
  - **Process risks** relate to processes employed to run the business.
  - **Compliance risks** cover complying with laws and regulations.
  - **People risks** relate to attracting and retaining key people, performance measurement, succession planning, communication, compensation.

- **Financial Risks:** Risks affecting the financial viability of the organizations:
  - **Budget risks** are the potential for the estimates or assumptions built into a budget to turn out to be inaccurate.
  - **Economy risks** are the probability that changes in the greater economy will negatively impact the organization.
  - **Accounting risks** are financial fraud or significant accounting errors.

- **Informational Risks:** Risks related to the compilation, analysis, and reporting of information that is key for decision-making:
  - **Financial risks** include information used or relied on for internal and external reporting (e.g., accounting, budgeting, financial reporting, and regulatory reporting).
  - **Operational risks** cover information used internally for understanding and evaluating operational effectiveness and efficiency.
  - **Technological risks** encompass information systems design, operation and control, availability of information, and use or exploitation of information.

Participants understood that they could consider many different risk categories and subcategories (see Exhibit D for more definitions and examples). As with all phases of risk assessment, they believed it was important to customize the risk categories to meet the organization's needs. For example, reputational risks are of outmost importance to OIG organizations. Therefore, participants included reputational risks as a subset of strategic risks. Once risk categories and

groups are determined, it can be helpful to depict the risk categories visually to help communicate and educate an organization's internal and external stakeholders.

ERM is a continuous, never-ending process, and all risks must be reassessed periodically to evaluate their future impact on their organizations' success. Participants noted operational, reputational, and cultural are the most prevalent risks to be addressed as they ramped up their ERM process. As with any ERM process, the risks and priorities may change as the organization's process becomes more mature. (See Exhibit E for other risks to consider.)

Risk Attitude

Participants stated that another important part of an effective ERM process is for senior management to articulate the organization's risk management philosophy, risk appetite and to understand the level of acceptable risk tolerance.

Risk Management Philosophy

COSO 2004 defines risk management philosophy as "the set of shared beliefs and attitudes characterizing how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities." Risk management philosophy defines the attitude to take on risks, which ranges from risk averse to risk aggressive. Each organization needs to determine where it lies within that range (COSO 2017). (See Figure 1.)

Figure 1: Risk Range

Participants developed or leveraged a leadership philosophy as a first step to reflecting their risk management philosophies. Some of those leadership philosophies were:

- We are a diverse organization of public servants dedicated to excellence and unified in helping the agency accomplish its mission to create strong, sustainable, inclusive communities and quality, affordable homes for all.

- We are motivated by performing essential, innovative, and influential work that addresses the agency's most significant management challenges.

- Because our work is often complex and without precedent, we leverage the diversity of our skills and experiences and take a participatory approach with the agency and other stakeholders to develop the best solutions. Trust and integrity are the foundation of our leadership approach. We do not ask of others what we would not do ourselves. We are approachable, empathetic, ethical, fair, transparent, and truthful. We say what we mean

and mean what we say. Our words and actions are in sync.

- Our service is a public trust. We are loyal to the organization and our people and operate with their best interests in mind. The needs of the organization outweigh our own aspirations.

- Our core values create an environment that fosters teamwork and open communications, empowers individuals to grow and take risks, and recognizes successes across the organization and the agency.

Risk Appetite

Risk appetite can be qualitative or quantitative terms that describe the amount and type of risk an organization chooses to accept in an effort to achieve its strategic goals and objectives. Descriptions of risk appetite should reflect the entity's culture. If an organization chooses to change some aspect of the culture, defining a strong risk appetite may help create and reinforce the desired culture (COSO 2017).

Participants leveraged senior management discussions, including strategic planning, and the risk identification and analysis phases of ERM to help define risk appetite and to articulate how much risk is acceptable relative to the risk appetite and specific goals and objectives of the organization. An assessment of risk appetite helps answer the question: How much risk is management willing to accept after careful consideration of risk versus reward? Understanding risk tolerance and the ability to manage the risks can help in developing choices and trade-offs. Failure to define and articulate risk appetite may result in employees making business decisions that are either too conservative (i.e., do not take on enough risk, which may result in unnecessary or excessive expenditure of valuable resources) or too aggressive (i.e., take on too much risk that could present unacceptable exposure to the organization).

Table 3 is a risk appetite rating scale adopted by some participants. They obtained the scale from GAO 17-63 *Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*. By understanding the risk appetite, risk tolerance, choices, and trade-offs, their organizations were able to better align their resources in pursuit of strategic goals and objectives, as well as to help define their organizational risk culture. (For more on risk culture appetite, see "Identifying and Improving Risk Culture" under "Sustaining ERM.")

Table 3: GAO's Risk Appetite Rating Scale

Rating	Risk Taking Philosophy	Tolerance for Uncertainty	Choice *When faced with multiple options, how willing are you to select an option that puts this strategic objective at risk?*	Trade-Off *How willing are you to trade off this strategic objective against achievement of another strategic objective?*
5 - Open	Will take justified risks	Fully anticipated	Will choose the option that offers the highest return, including accepting the possibility of failure	Willing
4 - Flexible	Will take strongly justified risks	Expect some	Will choose the option that includes risks, but will manage the impact	Willing under certain conditions
3 - Cautious	Preference for safe delivery	Limited	Will accept an option with limited risks that are heavily out-weighed by benefits	Prefer to avoid
2 - Minimalist	Intentionally conservative	Low	Will accept an option only if risks are essential, with limited possibility of failure	With extreme reluctance
1 - Adverse	Risk avoidance is a core objective	Extremely Low	Will select the lowest risk option, always	Never

Participants agree that there are a number of ways for an organization to define its risk appetite. It is up to leadership and management to communicate the risk appetite throughout the organization. Often, as an organization becomes more experienced in ERM, the organization's description of risk appetite becomes more precise. For example, as depicted in Figure 2, the risk appetite may also be expressed as a continuum (COSO 2017):

Figure 2: Risk Appetite Continuum

For the participants, risk appetite guides how an organization allocates resources, both throughout the entire organization and within individual components or operating units. The goal is to align resource allocation with the organization's mission, vision, and core values. Risk

appetite should be incorporated into decisions on how the organization operates at all levels of the organization.

Risk Tolerance

Closely linked to risk appetite is tolerance — the acceptable variation in performance (COSO 2017). Risk tolerance is a measure of the amount of variability an organization is willing to accept to pursue organizational goals and objectives. The level of risk tolerance is based on the organization's risk appetite. Often times the terms risk appetite and risk tolerance are used interchangeably, but they are two distinct concepts.

It is important to note that risk appetite is broad, while risk tolerance is tactical, focused, and related to organizational objectives and performance. For example, an OIG organization may have a low appetite for risks that may affect the timeliness of audits, but may tolerate some delays, if such delays could enhance the impact of an audit. In this case, the OIG organization may choose to develop a performance target to closely monitor the percentage of audits being issued on time (perhaps measured by the percentage of audits completed within 12 months of initiation), and evaluate any variability in accordance with their overall low appetite for risk. (See "Performance Management.")

Risk Assessment

Participants agree that a risk assessment requires answering the following key questions:

- What are the risks affecting OIG?
- What risks could affect attainment of OIG's strategic goals and objectives?
- What effect would those risks have on strategy, operations, reputation, compliance, reporting, and other key factors?
- How likely is it that those risks will occur and at what level of impact?

Before answering these questions, it is important to develop the criteria governing each risk under review, assessment scales, and a process for scoring and depicting results. The key is to develop risk criteria and categories that can be understood and foster consistent results. (See "Implementing ERM.")

Risk Rating Criteria

The exercise of determining the risk rating criteria and developing scales and a process for scoring should not be taken lightly. Common risk rating criteria used by the participants included the following:

- Impact: How significant are the potential consequences of the risk?
- Likelihood: How likely is it that the consequences will occur?
- Effectiveness of Management and Controls: What are the strengths of current risk mitigation and control activities already in place?
- Risk Velocity: What is the speed at which risks could impact the organization?

- Risk Tolerance: What is the organization's perception of tolerance for each particular risk?
- Persistence: If a risk should turn into an event, how long would it continue to affect the organization?
- Dynamic: Is the risk increasing, decreasing, steady, or volatile?

Risk Assessment Scales

Participants agreed that some form of measurement of risk is necessary. Without a standard of comparison, it is not possible to compare and aggregate risks across the organization or business unit. While most organizations define ***scales*** for impact and likelihood, scales can also provide the means to compare and aggregate risk velocity and risk tolerance. Every organization is different, so each should customize the scales to fit its size, complexity, and culture.

Participants recommended using a 5-point scale (versus a 3-point or 10-point scale) because it provides better distribution of ratings, thus facilitating the analysis and identification of top risks. (See the example under "Risk Appetite.")

Impact Rating Criteria

Participants address ***impact*** as the threat to the organization's ability to achieve its objectives and execute its strategies successfully. It is also common to think of impact in terms of effect on finances, reputation, regulations, health, safety, security, environment, employees, customers, and operations. Terms used by participants to define the rating scale for impact may include the following:

- incidental, minor, moderate, major, and extreme;
- insignificant, minor, moderate, major, catastrophic;
- no impact, minor impact, moderate impact, high impact, and very high impact;
- negligible, minor, moderate, major, and high; or
- very low, low, moderate, high, and very high.

It is helpful to assign a timeframe to impact. For instance, if the strategic objectives focus on a 4-year time horizon, management should consider risks within that period. The time may be longer for risks associated with the mission, vision, or strategy.

Likelihood Rating Criteria

Participants agreed that risks should be evaluated for two fundamental aspects: (1) ***impact*** of the consequences and (2) ***likelihood*** of the occurrence. After determining the consequences of a realistic worst-case scenario, the next question is: How likely is it that the consequences will occur? Likelihood can be expressed using qualitative terms; quantitative terms, such as a percent of probability; or, as a frequency. Like impact, the timeframe should be taken into consideration. Participants leverage the following terms to define the rating scale for likelihood:

- rare, unlikely, moderate, likely, and almost certain;

- rare, unlikely, possible, likely, and frequent;
- very low, low, moderate, high, very high;
- very unlikely, unlikely, possible, likely, and highly likely;
- almost impossible, extremely unlikely, possible sometimes, isolated incidents, repeated incidents; or
- never, unlikely, possible, likely, and definitely.

Participants said that scoring the impact and likelihood of risks requires a high degree of professional judgment, understanding of the effectiveness of internal controls, and familiarity with the risk rating scales. Table 4 includes examples of impact and likelihood rating scales.

Table 4: Impact and Likelihood Risk Rating Scales

Impact	Likelihood
(5) Very High: Degradation of an activity or role is **severe**, impacting our ability to meet one or more strategic goals, objectives; produce key deliverables; or reach required levels of performance to meet the mission.	**(5) Very High:** The risk event is almost **certain** to occur. Likelihood of occurrence is **90–100 percent.**
(4) High: Degradation of an activity or role is **major**, requiring immediate escalation or management intervention to reach required levels of performance of key functions.	**(4) High:** Risk event highly **likely** to occur. Likelihood of occurrence is **50–90 percent.**
(3) Moderate: Degradation of an activity/role is **moderate** with material impact on performance of key functions.	**(3) Moderate**: Risk event **possible** to occur. Likelihood of occurrence is **25–50 percent**.
(2) Low: Degradation of an activity/role is **minor**. It is noticeable and may affect performance of key functions.	**(2) Low:** Risk event **unlikely** to occur. Likelihood of occurrence is **10–25 percent.**
(1) Very Low: Degradation in activity or role is **negligible**, not expected to significantly affect performance of key function(s).	**(1) Very Low:** Risk event occurrence is **remote**. Likelihood of occurrence is **0–10 percent**.

Effectiveness of Controls Rating Criteria

Participants look to evaluate the strength of existing controls and risk management activities. This includes internal controls or responses (if any) currently in place to mitigate risks. Internal controls comprise of plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives. In short, internal controls help managers achieve desired results through effective stewardship of public resources. Participants apply this rating criterion after assessing inherent impact and likelihood, and it is used to determine residual scores for each risk identified (see "Inherent Risk and Residual Risk"). Terms used to describe effectiveness of controls include:

- no control in place, control in place but largely ineffective, not consistently effective, effectively mitigates risks most of the time, consistently and effectively mitigated risks and

- ineffective or ad hoc, somewhat ineffective, effective, very effective, extremely effective.

Table 5 shows an example of a rating scale for effectiveness of controls.

Table 5: Effectiveness of Controls Rating Scale

Score	Rating	Percentage Controlled
1	Ineffective or Ad Hoc	0%
2	Somewhat Ineffective	25%
3	Effective	50%
4	Very Effective	75%
5	Extremely Effective	100%

Risk Velocity Rating Criteria

Although not widely used, participants are rapidly adopting risk velocity as a risk-rating criterion**.** Risk velocity refers to the time it takes for a risk event to manifest itself. Knowing the time that elapses between the occurrence of an event and the point at which an organization first feels the effects of that event is useful when developing risk response options. To illustrate using an example from the weather, some risk events are felt immediately, such as the burst caused by a tornado, while others may take longer, such as delayed flooding from a hurricane. The thinking is that risk events that occur very quickly with little advance warning are inherently more difficult to react and respond to. Therefore, risk velocity is becoming a more common risk assessment criterion (Sobel 2015), and an element that most practitioners plan to incorporate in their frameworks. For example, one working group participant uses velocity, as well as likelihood and impact, to manage the risk associated with unimplemented recommendations. Velocity is used to assess the risk associated with the age of an unimplemented recommendation.

Table 6 shows an example of a risk velocity rating scale.

Table 6: Risk Velocity Rating Scale

Score	Rating	Description
1	Slow	Impact to materialize for more than 1 year
2	Moderate	Impact to materialize in 1 year
3	Rapid	Impact to materialize in 1 quarter

Scoring and Depicting Results

Participants score inherent risks by averaging impact and likelihood, the product of multiplying impact by likelihood, a weighted average, or some other formula. Effectiveness of controls should also be included in the calculations, often by multiplying the inherent risk by the percentage of the risk not controlled to derive the residual risk (see "Inherent Risk and Residual Risk"). Whether and how to round the results should be considered.

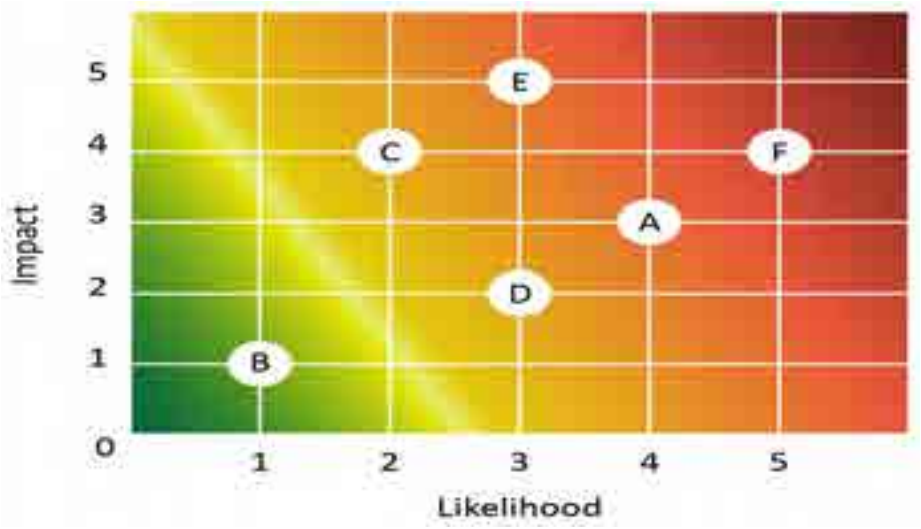
In addition to inherent and residual results, participants are in the process of factoring risk velocity and risk tolerance ratings into their results. This process can be helpful when selecting top risks, mapping out a holistic risk landscape, and fine-tuning mitigation activities.

Although there are multiple approaches to visually report risks, participants depict assessment results using a heat map to highlight the severity of each risk. The levels of severity may depend on the focus of the risk assessment. Common severity measures and color-coding schemes include:

- low (green), moderate (yellow), and high (red) or
- low (green), moderate (yellow), orange (high), and red (critical).

A simple way to view the results of a risk assessment is by plotting the relationship between impact and likelihood for each risk or risk category on a heat map. The size of the data points can be used to reflect velocity (onset). The boundaries between each level of severity depend on the risk appetite and tolerances. For example, Figure 3 depicts a heat map from one of the participants. Reflecting the mindset of most Federal agencies, the heat map depicts greater risk aversion with the risk appetite shifted to the bottom left. Specifically, the risk appetite line runs from an impact score of about 5.5 to a likelihood score of about 2.5. The area above and to the right of the risk appetite line is deemed to be sub-optimal and action should be taken.

Figure 3: Risk Heat Map



Participants depict risk results based on demographic information and other data. For example, based on the sample population and information collected, risk results can be presented by the organization's component (as shown in Figure 4), geographical location (i.e., headquarters or regions), seniority, etc. Strategic goals, categories, root causes (as shown in Figure 5), efficacy of internal controls, or other combinations can help depict risk results.

Figure 4: Risk Depiction by Component

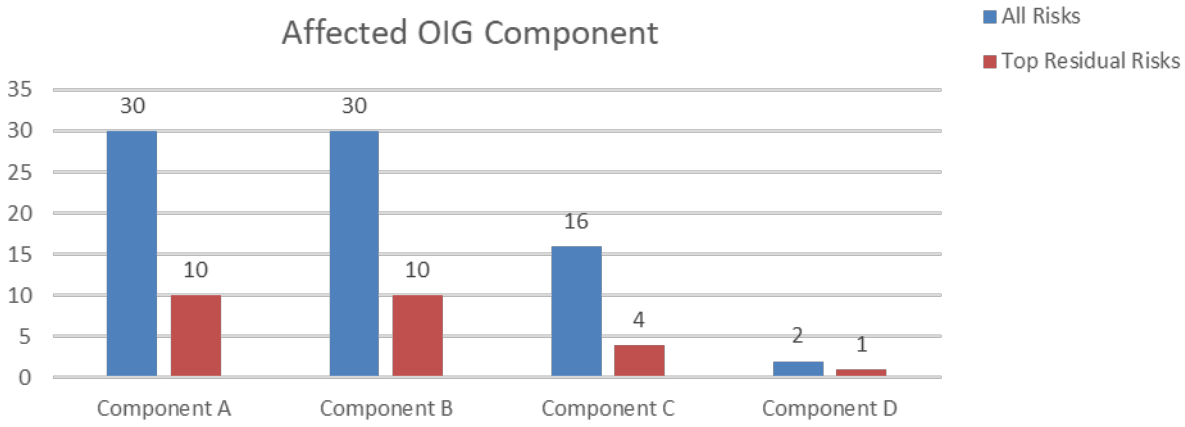
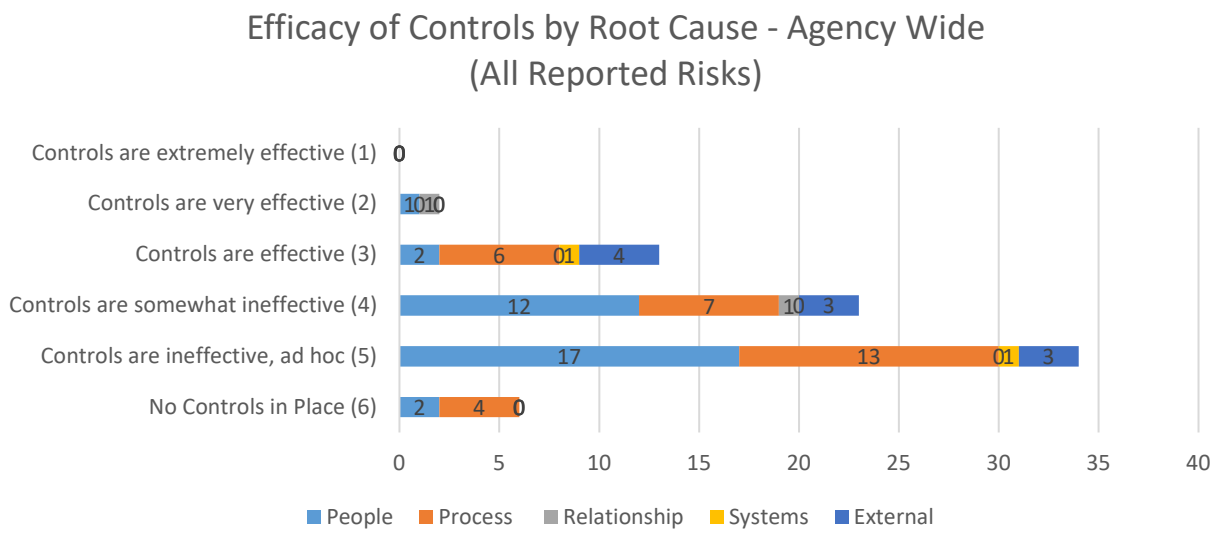


Figure 5: Risk Depiction by Efficacy of Internal Controls by Root Cause



IMPLEMENTING ERM

Participants agreed that the ERM implementation phase should not be taken lightly. Despite the planning and careful consideration that goes into developing the right ERM framework, the path to implementing ERM may at times be fraught with difficulties, a high level of stress, surprises, and at times, outright resistance. While proper planning is key, participants relied on a strong network of support and extensive benchmarking to navigate the difficulties associated with this phase.

Leveraging CIGIE, Federal Agencies (non-OIG), and Private Sector Networks

Participants consulted with CIGIE, other Federal agencies (both OIG and non-OIG), and private sector entities to identify good practices, to better understand the external environment, and to stay abreast of the latest ERM trends. In fact, the *ERM Playbook* notes that a key duty and responsibility of the CRO is to establish and maintain "close and continuing contact and effective liaison with [agency] policy offices and bureaus, congressional and agency staffs, and high-ranking representatives of the financial community, consumer and community organizations, and other government agencies, and government officials." However, in an effort to preserve OIG independence and objectivity, participants stated the need to be mindful and refrain from substantial involvement, or from shaping ERM programs, within the agencies they oversee.

During their implementation efforts, participants leveraged non-OIG networks with Federal agencies (mostly outside the agencies they oversee) to benchmark ERM implementation activities. A 2016 GAO report entitled *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*[14] offered a reference point for identifying agencies with more mature ERM programs that could be contacted for benchmarking purposes.

Although participants mentioned that some agencies may have been initially hesitant to share their practices with OIG personnel, with time and meaningful interactions, most agencies were open to sharing their good practices. Moreover, OIG organizations may want to consider engaging in constructive coordination with agency management to explore a consistent approach to manage potential *Freedom of Information Act* (FOIA) requests. Fortunately, thanks to efforts undertaken by the Partnership for Public Service, the Association for Federal Enterprise Risk Management (AFERM) and Association of Government Accountants (AGA) in the last few years, significant progress has been made in creating a strong ERM practitioners' network across Federal agencies. AFERM's website includes a robust set of ERM reference materials.

Another nonprofit entity that has provided extensive networking opportunities is the Society of Corporate Compliance and Ethics (SCCE).[15] SCCE's stated mission is to "champion ethical practice and compliance standards and to provide the necessary resources for ethics and compliance professionals and others who share these principles." Specifically, a number of participants are certified as Corporate Compliance and Ethics Professionals (CCEP) by this

[14] https://www.gao.gov/assets/690/681342.pdf
[15] https://www.corporatecompliance.org/AboutSCCE/AboutSCCE.aspx

organization. They frequently attend live and online SCCE-sponsored training, events, seminars, and podcasts.

Within the OIG community, in 2018 the CIGIE Professional Development Committee (PDC) formally adopted the ERM working group.[16] The CIGIE PDC's objective is to provide educational opportunities through the CIGIE Training Institute for members of the OIG community and ensures the development of competent personnel. Accordingly, participants leverage these venues to share any innovations in ERM, so that other OIGs may benefit from such communal knowledge.

Finally, participants leverage publications about ERM implementation in the private sector or take advantage of ERM subscription services to access templates and resources. Private firms can offer a wealth of historical and contemporary global knowledge, which OIGs should leverage as they continue on their ERM journey. By evaluating their current risk-management activities in contrast to good practices in the private sector, participants try to avoid pitfalls and to identify areas for potential improvement.

Record Keeping of Enterprise Risk Management Materials

Prior to undertaking risk identification, analysis, and mitigation activities, participants consulted with OIG attorneys, records management officials, and FOIA officials, to determine potential implications of existing disclosure laws given the sensitivity of the information gathered as part of the ERM process. Organizations must understand FOIA requirements and ensure materials are safeguarded and properly marked. In some cases, ERM pre-decisional and deliberative materials that reflect personal opinions rather than agency policy may be subject to a non-disclosure privilege under FOIA. If so, this may allow for open and frank discussion on matters of policy between subordinates and superiors. Attorneys, records management officials, and FOIA officials should be consulted for clear guidance.

Risk Management Discussions with Your Agency

Participants have engaged in ERM discussions with the agency they oversee. However, a number of agencies have yet to establish a formal ERM process or have very limited development. In these cases, discussions focus on benchmarking, or sharing of good practices, as ERM implementation activities are undertaken.

Conversely, several participants regularly consult with the agencies they oversee, in particular the executive team or CRO to the extent that they have a mature ERM program. In some cases, these agencies have provided their risk profiles to their OIGs and have invited them to attend recurring ERM meetings. Agencies have also requested input regarding how OIGs develop their top management challenges. Similarly, participants have allowed their financial audit group to work with the agency's CRO and Chief Financial Officers to identify controls related to their work. In other cases, OIG sits on the agency's ERM working group.

[16] https://www.ignet.gov/content/professional-development

Regardless of the chosen ERM approach, participants emphasized the need to be cognizant of OIG's independence obligations. To this end, an informal rule-of-thumb for ERM (as with many operational matters) has been "cooperation not collaboration."

Other recommendations include:

- Liaisons or champions (at the working level) are essential to implement and build ERM capacity from the ground up.
- Consider OIG's Top Management Challenges, GAO's High-Risk List, CIGIE's Crosscutting Risks, and other potential areas of risks related to shared services.
- If an agency requests details regarding specific OIG's risks, it is acceptable to decline given the need for independence.
- Check with your Records Management Officer to identify any FOIA exclusions of ERM inputs and outputs.
- Consider establishing a new set of parameters with your agency to encourage free flow of information about the agency's risks. Parameters should take into account and evolve based on agency's level of ERM maturity.
- Leverage the Federal Employee Viewpoint Survey (FEVS) results to gauge agency risk culture. Understanding the risk culture can help uncover (among other insights), how comfortable staff are with raising concerns to leadership and that leadership will take appropriate actions to respond to those concerns.

Identifying Risks

As part of their ERM implementation efforts, participants employed numerous techniques to identify risks within their organizations and to develop a risk register and profile to conduct analyses.

Approaches for identifying risks include top down (leveraging senior management to identify risks) or bottoms up (leveraging staff at all levels). Approaches also include using in-person interviews, surveys;[17] reviews of GAO reports or reports of other OIGs to identify risk trends; reviews of internal incident reports; and regular (generally semiannual) consultations with OIG Ombudsmen, budget, employee advisory, EEO, and upper management staff. FEVS data, organizational performance and budget information, and quality assurance reports also provide invaluable risk information. Together, these sources are able to identify organizational risks over a wide spectrum of risk areas.

Participants used more than one of these mechanisms and preferred in-person interviews to collect risks during the initial maturity stages. Once an organization advances in its ERM maturity, other methods, such as surveys, can be considered. Surveys can be particularly useful

[17] See "Sustaining ERM" for additional discussion.

to rate and rank predetermined emerging risks. Regardless of the method for identifying risks, participants warned of falling into the trap of reporting too many risks, which can limit the organization's ability to analyze and prioritize the most significant risks.

Participants also agreed on the importance of identifying personnel to support the interviews as part of the risk identification and, potentially, the analysis process. Depending on the sample size, it may be necessary to identify certain individuals as risk liaisons or risk champions within components to help facilitate interviews, collect risks (especially if leveraging a bottom up approach), and determine patterns. Ideally, these individuals should possess an interest in risk management, interpersonal skills, and analytical skills. These individuals should agree to maintain confidentiality and be very familiar with the ERM framework. Risk liaisons can help point out differences in risk language or assessment methodology across components that may lead to redundancies or blind spots in the enterprise risk portfolio. They can also identify areas where interviewees or stakeholders disagree about the amount of risk the organization should take.

Planning In-Person Interviews

When choosing in-person interviews, participants agree that it is important to dedicate enough time to identify potential interviewees, accommodate scheduling of meetings, facilitate meetings, and consider other logistical issues. It is also valuable to identify a cross section of the organization for interviews, including headquarters and regional staff, leaders, managers, and non-managerial staff. Participants emphasized the need to be transparent with interviewees from the beginning. In particular, interviewees should understand the reason why they are being interviewed, the process of selecting individual employees for interviews, and how their contributions will assist in identifying, analyzing, and mitigating risks.

In the case of broader risk assessments that are enterprise-wide and relate to all types of organizational risks, a greater number of employees could be interviewed. However, all participants in some way limit the number of employees interviewed, not to limit the chance to obtain and provide input, but to be able to manage the volume of interviews. (It is not feasible to interview every employee in the organization in every single risk assessment.)

For specialized risk assessments (focusing on a discrete area of risk such as data privacy or procurement/contracting), the interviews can be limited to subject matter experts (SME) in that field.

Narrowing the number of interviews can be accomplished in several ways; here are a few options identified by the working group:

- Interview a randomly selected 10 percent of all employees semiannually between meetings of the RMC to identify or update risks.

- On risk assessments limited to one or a small number of risk categories, focus on interviewing SMEs within OIG who are knowledgeable about those specific risks; identify them by asking the AIGs/executives in OIG.

- In risk assessments that seek to identify all risks in an organization, interview a combination of supervisors (GS 15-level) and other employees with both supervisory and non-supervisory responsibilities. The idea is to get a cross section of input, not only from executives and managers but also from a broader base of all OIG employees.

Conducting Interviews

Among participants, there is consensus that written questions with interview instructions should be sent to employees before the actual interview, in particular during the early ERM maturity state. Interviewees should be instructed to review the ERM framework to understand the approach, risk categories, risk rating scales as well as instructions and questions, which are then used as a springboard for a broader discussion during the actual interview. Participants said that they do not simply read the questions and collect an answer—a broader discussion about most significant risks gives better insight into potential ranking and mitigation for each risk reported. For better understanding and efficiency, it is important that everyone come prepared for the interviews.

The instructions should inform the employees why they have been selected and the purpose of the interview. The instructions should also define key terms—for example, if the employee is asked to give a root cause(s) for a particular risk; the concept of root cause should be explained and defined.

Participants recommend the interviewers stress that interviews should focus on high-level, enterprise-wide risks that could affect the achievement of strategic goals and objectives. Interviewees should be able to identify key risks (based on the risk categories defined in the ERM framework), explain how those risks affect the ability of the organization to accomplish strategic goals and objectives, and explain the impact and likelihood based on the established methodology. Based on participants' experiences, questions that could be asked during the interviews include the following:

- What are the three to five top risks to achieving the OIG's strategic goals and objectives?
- Specifically, what strategic objectives are affected by these risks?
- What OIG component(s) is being affected?
- What risk categories apply to those risks (strategic, operational, reporting, compliance, etc.)?
- What is the root cause for those risks (internal, external, people, process, systems, etc.)?
- What is the cause and effect of those risks?
- If the risks were to occur, what would be the impact/likelihood?
- What controls or management responses are currently in place to address the risks?
- How effective are those controls or management responses?
- Should we accept the risk? Is further action needed?
- What could be done to mitigate the risk?

Still, it is possible that interviewees will wish to discuss other issues that do not involve enterprise risks, such as an individual personnel matter or grievance. While these are not issues germane to the ERM process, it is important that employees receive advice on what they should do in such instances. Participants recommend developing a process beforehand that deals with

non-ERM complaints/issues that may emerge during interviews. This may include referral to OIG's Hotline, Ombudsman, Labor Employment Relations, EEO manager, Employee Advisory Council, etc. You may wish to consult with your Office of Counsel for their advice on how to handle non ERM-concerns brought up by employees prior to embarking on face-to-face interviews. Your counsel may also be able to give you guidance on how to handle protected disclosures during interviews, such as whistleblower complaints.

Transparency is an overarching issue for ERM. Participants stated that, at every opportunity in the process, you should explain what you are doing and why. Because interviews require the personal involvement of OIG personnel across the board, transparency is particularly important in this area. Use whatever mechanisms you can—blog entries, workshops, and meetings with your RMC and other employees to explain the purpose of their interviews—to ensure understanding of the interview process and in a larger sense to get the risk management message across. Building a culture in which risks are reported without fear of retaliation is an important ERM goal.

Other recommendations include:

- To the extent practicable, interviews should be conducted in person (or via video capability such as WebEx or Adobe Connect), in particular during the initial ERM maturity stages. In-person interviews will promote greater understanding of the ERM process and help build trust.

- Combining interviews with other risk identification mechanisms, such as surveys, is an effective strategy in risk identification. Surveys can be used to engage a larger number of people in the organization. Surveys should be as specific as possible to avoid responses not relevant to the risk assessment at hand.

- Consider offering anonymity to employees reporting ERM risks; some employees may feel more comfortable with this approach and this may increase participation in the risk assessment process.

- Ask about the root cause and consequence for particular risks, as well as proposed mitigation for that risk. This will help assess effectiveness of mitigation activities later on.

- Ask interviewees to focus on only the top three to five risks to achieving strategic goals and objectives.

Aggregating and Analyzing Risks

Participants shared that after identifying risks through interviews or surveys, it was essential to aggregate the information into a comprehensive risk inventory or register. This step allowed participants to understand risk events and drivers by components, strategic goals and objectives, sources, and probability of the risk occurring based on the criteria established in their ERM frameworks.

Participants leveraged aggregated risk data to find patterns between components and the OIG as a whole, and to analyze and evaluate risks based on assessments of impact and likelihood of identified risks in an effort to develop a ranked risk profile.

Participants also leveraged Excel to aggregate risks, leveraging the following data fields for each risk identified:

- Risk category
- Strategic objective affected
- Risk root cause
- Component affected
- Risk title
- Risk description (what could go wrong, including cause and consequence)
- Inherent impact and likelihood scores
- Description of current controls
- Residual impact likelihood scores
- Recommended mitigation strategies

Inherent Risk and Residual Risk

According to OMB Circular A-123, inherent risk is "the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations." There is risk in everything we do, and inherent risk can be seen as the risk of doing business. Organizations use the scales established in their ERM frameworks to assign measures for the inherent likelihood and inherent impact of each risk on the register. The inherent risk assessment does not take into account the effectiveness of current risk responses or existing controls. Participants noted that it could be difficult to measure inherent risk because internal controls are so deeply embedded into many activities. Ultimately, inherent risk is calculated as a product of inherent impact and inherent likelihood.

Residual risk, according to OMB Circular A-123, is "the exposure remaining from an inherent risk after action has been taken to manage it, using the same assessment standards as the inherent assessment." Prior to measuring residual risk, the effectiveness of existing internal controls must be identified and considered in terms of how effectively they mitigate risk. Written policies and procedures, results of manager reviews and monitoring, Peer Review Reports, and internal quality assurance reviews can be used to determine how effectively internal controls mitigate risks. Similar to inherent risk, residual risk is calculated as a product of residual impact and residual likelihood using scales established in the ERM framework. Residual risk levels are compared against the organization's risk appetite, as articulated in the ERM framework to determine whether additional action is needed.

Developing a Risk Profile

Once they compiled the risk register, participants developed numerous methods, processes, and tools to analyze and evaluate the risk inventory. While the methods have varied, the final deliverable is a risk profile. Keep in mind that a risk profile is different from a risk register or

inventory. The former is a prioritized inventory of the most significant risks as identified in the risk assessment process. (See "Analyzing Risks.") The latter constitutes a comprehensive inventory of risks. Both documents should be updated on a periodic basis as determined by the RMC (e.g., semi-annually, annually, biennially, or ad hoc).

Participants agreed that the objective of a risk profile is to enable analysis of the risks faced by OIG organizations as they conduct activities in pursuit of strategic goals and objectives. By aggregating and prioritizing risk information gathered through the identification phase, participants are able to understand key risks for their organizations.

There are several ways to develop a risk profile. Based on OMB Circular A-123 guidance, agencies have discretion in terms of the appropriate content and format for their risk profiles. However, as recommended by OMB Circular A-123, participants developed risk profiles that included the following elements:

- strategic goals and objectives affected by the risk, including the risk category;
- definition of the risk;
- inherent risk assessment (product of likelihood and impact before taking into account effectiveness of controls);
- existing risk response (current risk response strategies);
- residual risk assessment (after taking into account existing management controls);
- proposed risk response (including monitoring activities); and
- proposed mitigation plan (to further reduce the residual risk).

For further information on these components, practitioners should review the *ERM Playbook for the U.S. Federal Government.*[18]

Additionally, as a precursor to the risk profile (during the ad-hoc or initial stages of ERM maturity), participants worked on discreet projects through which risks were uncovered. In these situations, participants conducted a root cause analysis of specific programs or operations and provided recommendations to address the risks that were uncovered. They often conducted interviews and surveys and then presented their results to the RMC and senior leadership.

Approaches for Developing a Risk Profile

Some commonly used approaches for developing a risk profile include further organizing risks under themes based on risk categories and risk frequency. Risk themes include broad categories such as budget and resources, data integrity and security, human capital processes, organizational culture, audit timeliness, succession planning, and quality products and services. It is important to have common organizational definitions, including a methodology for organizing risks into themes to help avoid any confusion. The risk categories are intended to treat risks as potentially interrelated and not stove-piped within an individual component.[19] In the analysis process, practitioners should recognize that some risks might fall into multiple categories. The risk frequency approach is used to prioritize risk based upon the frequency of its occurrence and the

[18] https://cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-*Playbook*.pdf

[19] See Exhibit D for definitions and examples.

related consequences if left unmitigated. In addition, these organizational approaches are often employed separately or in tandem with other evaluation strategies to identify the organization's top risks for the risk profile.

Once the suitable organizational approach is determined, participants use a risk profile tool to accomplish many of the following objectives:

- document the chosen organizational approach(es)—theme, category, frequency;
- assess the associated risk impact and likelihood of occurrence;
- evaluate the efficacy of any controls for the risk;
- identify top risks as previously chosen by leadership or based on the OIG's risk appetite;
- annotate responsible persons/components for managing the risk;
- document mitigation strategies (both short and long term); and
- monitor and evaluate actions taken.

Regardless of how often risk inventories or profiles are updated, practitioners must be agile and identify emerging risks raised through the RMC (or similar leadership venues), staff, media, academia, etc.

Analyzing Risks

Participants agree that evaluating and prioritizing risks that have the most significant impact on OIG is key to determine where to focus treatment efforts. There are several approaches for analyzing and identifying risks, but most participants choose to engage internal stakeholders through focused meetings, workshops, or working groups composed of staff (preferably volunteers) from across OIG. Examples of approaches include:

- single meetings (one or two day-long meetings) to identify top risks, especially those within a finite time span (rapid velocity), and emerging risks; or

- a series of short meetings (an hour or two) to analyze risk information gathered through other means, validate assumptions, and identify emerging risks, if need be.

The duration of the meeting(s) should be set according to the desired outcome, participant schedules, and other constraints. Participants also leveraged crosscutting working groups to conduct analysis of risks and recommend mitigation activities. The working group met in a series of meetings to discuss the risk root drivers (causes) and possible outcomes (consequences) as they analyzed risks by using a casual factor diagram analysis (that information was then used to rank risks). Figure 6 provides an example of a causal factor diagram.

Figure 6: Causal Factor Diagram Example

Moreover, as the organization matures in its ERM practices, practitioners may want to consider the risk interdependencies for a better understanding of risk definitions and degree of impact risks have on each other.

Participants said that significant pre-work is required in advance for these meetings, including managing logistics, developing charts summarizing initial risk findings based on the risk identification phase, and developing risk information based on stakeholder needs. Finally, ownership of the risk mitigation plans must be assigned to processes or to risk owners to make them accountable for mitigation strategies.

Implementing Risk Appetite

Participants shared that in the early maturity stages, organizational risk appetite could be better understood and defined after identifying risks, completing a risk register and profile, and conducting risk assessments. After the risk appetite is identified, the next objective is to focus on drafting clear risk appetite statements and understanding risk tolerance.

Other recommendations for implementing risk appetite include:

- Leverage risk appetite statements, performance metrics, and tolerance levels from components to understand the current risk appetite or posture.
- Share iterative drafts of the risk appetite statements with senior management before deciding on a final version.
- Test whether the risk appetite statements are clear and useful across the organization.
- Seek approval of the statements from stakeholders and leadership to gain buy-in and drive accountability.
- Look to improve each year from the previous ERM cycles. Consider using "risk scenarios" to identify risks when interviewing staff.

- Keep in mind that OIGs may develop or understand their risk appetite, as they develop their risk assessments, not necessarily before. OIGs want to start seeing a picture of their risk universe in order to understand and inform their risk appetite and make modifications, if necessary.

- Where possible, tie organizational performance indicators to risk tolerance.

Leveraging the Risk Profile to Enhance Internal Controls and Decision-Making

As previously mentioned, participants strongly recommend leveraging the risk register, profile, and risk analysis discussions to understand the current organizational risk posture, including effectiveness of internal controls and decision-making. By understanding and documenting how the organization currently considers and addresses risks, it will be easier to identify inconsistencies between the OIG risk-taking appetite and current internal controls. This can be done by understanding OIG and component policies or directives, past leadership decisions, group and component-level initiatives, organizational norms, and key performance indicators (KPI) or operational metrics. Some questions to consider include:

- Where does our organization document its goals and expectations?

- How do we determine whether we have met our goals and expectations (metrics)?

- How effective are our current policies and procedures at addressing risks?

- What are a few recent instances in which risk considerations influenced a number of key decisions?

- In your view, where do we not meet expectations? What evidence is there?

By understanding the efficacy of internal controls, participants were best positioned to identify areas of potential weakness and recommend improvements. For example, many risks could stem from staff's misperceptions about internal controls or outdated policies and procedures.

Some participants work closely with their Quality Assurance Review (QAR) functions to identify risks and enhance internal controls. Several OIG organizations have a separate internal (quality assurance) office charged with conducting independent reviews by staff not assigned to the unit being reviewed. The CIGIE Peer Review system is yet another layer of external quality assurance available to OIG organizations.

Given the expansive nature of quality assurance activities in the OIG community, both internal and external, practitioners should continually leverage the results of all relevant activities as they establish and mature their ERM capabilities. It is important to note that the ERM function does not have to be entirely separate from the internal quality assurance program. However, the quality assurance staff involved in ERM must consciously maintain an appropriate and

transparent level of independence to ensure that any future quality assurance reviews of ERM capabilities are free, both in fact and appearance, from any conflicts, bias, or impairments.

Other recommendations for leveraging the risk profile include:

- Consider the efficacy of internal controls by reviewing prior quality assurance reports.
- Collaborate with QAR staff to develop an annual review schedule that considers ERM risk assessment results. (Risk assessment results may also be considered during the planning of individual quality assurance reviews to help inform the scope and coverage period of the review.)

ERM risk assessment results, quality assurance review results, and self-assessment on internal controls performed by each OIG component may also be used to support annual FMFIA assurances on internal controls.

Visualization Options

Many visualization tools are available to support the development of risk inventories and profiles. Such tools can depict and compare individual risks and identify trends across risk categories, residual scores, and other parameters. The best tools may be customized to fit agency-specific needs. However, the most common visualization options include charts, graphs, dashboards, diagrams, and heat maps.

At the more mature levels of ERM implementation, crosscutting teams of volunteers are formed to rank risks for additional perspective before they are presented to the risk council. In this way, the risk council considers their ranking when making decisions of its own. Some participants shared that individual risk owners rank risks because they are expected to have to address risk assumptions. A particular participant stated that her risk profile spreadsheet depicted top risks (i.e., Top 10) along with directional arrows depicting whether a risk has trended up or down from the previous year.

Leveraging Other Data Sources

Participants also strive to connect the dots with other relevant data sources when identifying the risk profile. For example, the FEVS,[20] a tool that measures employees' perceptions of whether, and to what extent, conditions characterizing successful organizations are present in their agencies, may serve as a prime source of quantitative and qualitative data elements to inform risk indicators. Similarly, some participants have historically used the U.S. Office of Personnel Management's (OPM) Organizational Assessment Survey (OAS)[21]—in off years from the FEVS survey—to track the aforementioned trends in workforce satisfaction. Others plan to use measures and FEVS responses to develop appetites and tolerances to determine whether action is needed, or to develop key risk indicators. According to OPM's website, "Currently..., 5 CFR Part

[20] https://www.opm.gov/fevs/
[21] https://www.opm.gov/policy-data-oversight/data-analysis-documentation/employee-surveys/buy-services/organizational-assessment-survey/

250, subpart C, requires executive agencies to conduct an annual survey, and when the FEVS is administered, OPM fulfills this obligation for agencies."

Participants have also drawn risk data from unconventional sources, including Partnership for Public Service rankings; peer reviews; risk culture pulse surveys; GAO reports; CIGIE's crosscutting list, Top Management Challenges; succession planning/personnel data; and organizational performance results.

Responding to Risk

After identifying and assessing risks, organizations must select and deploy a risk response. Consideration should be given to the severity and prioritization of the risk (COSO 2017), as well as strategic objectives, organizational performance targets and resource availability. There are various types of response options to risk, including:

- Assume: Acknowledge the existence of a particular risk and make a deliberate decision to accept it without engaging in special efforts to control it. Approval of management should be required.

- Avoid: Adjust requirements or constraints to eliminate the risk. This adjustment could be accommodated by a change in funding, schedule, or requirements. Choosing avoidance suggests that the organization was not able to identify a response that would reduce the risk to an acceptable level of severity (COSO 2017).

- Pursue: Seek an increased level of risk in an effort to enhance organizational performance. When choosing to pursue risk, management understands the nature and extent of any changes required to achieve desire performance while not exceeding the boundaries of acceptable risk tolerance (COSO 2017).

- Reduce/Mitigate: Manage the risk by undertaking activities to lower or reduce the significance or likelihood of a given risk, such as establishing controls to mitigate the risk.

- Share/Transfer: Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk (COSO 2017).

Participants shared that OIG organizations tend to choose risk reduction or mitigation options when responding to risk. Risk mitigation action plans are commonly leveraged to help their organizations move the identified risks into tolerance and promote accountability. Some participants post OIG action plans (related to each risk) on the OIG's community SharePoint page or their intranet to promote transparency.

However, several participants have not progressed beyond the analysis phase. Therefore, monitoring and action planning are still works in progress. For those organizations that have begun monitoring and action planning, establishing consistent documentation to standardize risk response plans, as well as developing dashboards to communicate progress during RMCs are key activities.

Developing Risk Mitigation Plans and Progress Monitoring

Risk mitigation plans are essential to improving organizational capacity to address risks that could affect the strategic objectives. Participants agreed that a first step to effective risk-response plans across the organization is to ensure stakeholders understand their responsibilities in carrying out risk response options. Although writing consistent criteria for developing mitigation plans is vital, it can prove very challenging, given the diverse perspectives of risk owners. Fortunately, with careful planning, ERM can help standardize the mitigation, assessment, and monitoring process.

Participants also leveraged working groups to conduct both risk analysis and formulation of risk mitigation activities. Because the working groups spent considerable time analyzing causes and consequences for risks, they were uniquely positioned to recommend mitigation strategies to risk owners. Recommendations were reviewed and prioritized by the RMC based on level of effort, benefit, and risk rankings.

Monitoring Risk

A risk monitoring effort or activity is a *push tactic* that empowers all employees to disclose, within their levels of oversight, the occurrence of a critical control point indicating a potential out-of-control situation or any potential risk events that could affect the enterprise. Consistent monitoring and review is necessary to ensure key controls and mitigation efforts remain appropriate and are implemented. In addition, by identifying leading or lagging key risk indicators (KRI) for top risks and defining risk tolerance levels for the organization, ERM practitioners can ensure risks are monitored consistently and effectively.

Practitioners can use a number of approaches to assign risk ownership and monitoring. One participant helped assign and monitor risks based on themes and agreed-upon mitigation strategies outlined in the action plans. Another participant offered the opportunity for leadership to volunteer and accept ownership because most of their risks were policy and procedure related and too much for one office to do alone. A third participant assigned ownership to the business office in which the risk was present. For example, the administrative function within the organization owns the risks pertaining to government contracting.

Organizations with mature ERM programs use KRIs to track early signs of risk exposure. Although this is an important area of risk management, for some participants this is still a work in progress. However, participants are taking steps to identify underlying root causes of the risk exposure and to develop risk thresholds and KRIs by collaborating with SME and risk owners. Table 7 provides examples of KRIs and thresholds.

Table 7: Example Key Risk Indicators and Thresholds

Risk Issue	Risk Category	Key Risk Indicator	Goal	Risk Thresholds
Outdated internal controls	Operational	Percentage of Inspector General Directives evaluated annually	Greater or equal to 80%	**Under 70%:** Significantly increasing risk level **Between 70 and 80%:** Moderately increasing risk level **Above 80%:** Comfortable with risk level

To help ensure risk owners (typically senior management) are held accountable, leadership is generally informed of risk management performance frequently during regularly scheduled meetings with the IG, RMC, and Quarterly Performance Reviews (QPR).

Assessing Risk

The *pull approach* is the risk owner's assessment process in which risk owners are periodically surveyed to assess whether risk mitigation plans are effective and to identify emerging risks and internal controls. Ultimately, the responsibility for risk management lies with the organization's leadership, managers, and the RMC. The accountable risk owners reported by participants are usually in leadership positions with responsibilities for risk management trickling down the management chain. Although each leader (and the leader's subordinate managers) is responsible for managing the risk in his or her area, the panel strongly emphasized the need for recurrent independent reviews that evaluate the program's adequacy to protect enterprise assets, reputation, and ongoing operations. In addition, outstanding gaps or observations should be appropriately communicated to the workforce.

INTEGRATING AND EMBEDDING ERM WITHIN ORGANIZATIONAL CULTURE AND OTHER PROCESSES

Fraud Risk

For purposes of this section, fraud risk will include fraudulent financial reporting, misappropriation of assets, acquisition/contract fraud, and corruption such as bribery and other illegal acts. Such risks may result in the theft, loss, or diversion of U.S. Government funds, property, or other assets. Practitioners should be cognizant of fraud risk as they assess other general areas of risk and integrate and embed ERM into the organizational culture and other processes (COSO 2017).

Principle 8 of the Green Book states that when management is identifying, analyzing, and responding to risks the potential for fraud should be considered. When implementing this principle, the following attributes contribute to the design, implementation, and operational effectiveness of this principle: types of fraud; fraud risk factors; and, response to fraud risk (Principle 8 – Assess Fraud Risk-GAO-14/704G *Federal Internal Control Standards*).

Fraud Risk Factors

Accordingly, practitioners are encouraged to consider fraud risk factors as they integrate and embed an ERM capability. The following fraud risk factors are granted special emphasis in the Green Book (Principle 8.04):

- **Incentive/pressure** - Management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud.

- **Opportunity** - Circumstances exist, such as the absence of controls, ineffective controls, or the ability for management to override controls, which provides an opportunity to commit fraud.

- **Attitude/rationalization** - Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

These factors are not indications of fraud, but they are usually present when fraud exists. The practitioner's process for analyzing fraud risk should be the same as the process that we performed for analyzing risks, and it should be part of the risk assessment process. The process' design should include actions for responding to fraud risk. Fraud risks may be reduced or eliminated with changes to activities and processes. As noted in Principle 8.07, changes may include "stopping or reorganizing certain operations and reallocating roles among personnel to enhance segregation of duties." The risk assessment process may also require revision if there has been a detection of fraud.

GAO Framework for Managing Fraud Risks

In July 2015, GAO published *A Framework for Managing Fraud Risks in Federal Programs* (the Fraud Framework) (GAO-15-593SP) to aid agencies in managing fraud risks. To guide agencies and OMB in their efforts to reduce fraud risks, Congress enacted the *Fraud Reduction and Data Analytics Act of 2015* (Public Law 114-186, June 30, 2016) (FRDAA), which created expectations for agencies to establish financial and administrative controls for managing fraud risks. In 2016, OMB A-123 was updated to reflect the guidance required by the FRDAA.

FRDAA requires agencies to (1) use a risk-based approach to evaluate fraud risks and implement financial and administrative controls to mitigate such risks; (2) collect and analyze data to monitor fraud trends and improve fraud prevention controls; and (3) use the results of monitoring, evaluations, audits, and investigations to improve fraud prevention, detection, and response.

FRDAA also requires agencies to publish in their Annual Financial Report a progress report ("Fraud Reduction Report") on their efforts concerning FRDAA. Specifically, agencies should:

A) implement the 1) required financial and administrative controls noted above; 2) GAO Green Book fraud risk principles; and 3) A-123 with respect to leading practices for managing risk;

B) identify risks and vulnerabilities to fraud, including with respect to payroll, beneficiary payments, grants, large contacts, and purchase and travel cards; and

C) establish strategies, procedures, and other steps to curb fraud.

OMB's Perspective on Fraud

OMB Circular A-123 requires agencies to integrate risk management and internal control functions. The Circular also establishes an assessment process based on GAO's Green Book (*Standards for Internal Controls in the Federal Government*) that management must implement in order to properly assess and improve internal controls. The Circular implements and elevates Principle 8 (Assess Fraud Risk), providing guidance as required by the FRDAA, which requires management to consider the potential for fraud risk when identifying, analyzing, and responding to risks.

In addition, OMB Circular A-123 provides an overview of GAO's Fraud Framework, and states that agencies should adhere to the leading practices of the Fraud Framework. The framework's objective is to assist managers with combating fraud and preserving government agencies' and program integrity. GAO developed the Fraud Framework by identifying good practices used across the Federal Government for managing fraud risks. GAO recommends that managers should consider using these good practices as part of their endeavor to effectively design, implement, and operate their internal control system. Managers are also responsible for determining the extent to which the leading practices in the Fraud Framework are relevant to their programs and for tailoring the practices to align with the program's operations.

Agencies must consider fraud risks in their strategic plans and ensure Federal officials involved in planning for, awarding, and managing grants and other forms of financial assistance receive training on fraud indicators and risk. The Circular asserts, for grants and contracts, that agencies should provide training on fraud awareness, identification, prevention, and reporting.

OMB's *Emergency Acquisitions Guide*[22] states that contracting officers should be familiar with common fraud indicators, including frequent customer complaints about poor quality or supplies or services, an abnormal increase in supply items, tools, and individual equipment.

To assist managers with mitigating fraud risks, the Fraud Framework includes control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risk. In addition, the Fraud Framework highlights the importance of monitoring and incorporating feedback, which are ongoing practices that apply the following segments:

- Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
- Plan regular fraud risk assessments to determine a fraud risk profile.
- Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.
- Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.

Another area addressed by the Fraud Framework is establishing risk tolerances in disaster situations. When determining risk tolerances in disaster situations, managers must continually balance meeting the program's operational objective versus reducing the likelihood of fraud. The Fraud Framework calls for managers to determine risk tolerance when assessing fraud risks and use that determination as part of the basis for developing responses. The Fraud Framework also includes a reference to additional guidance from the AGA *Fraud Prevention Tool Kit*.

Leveraging Disparate Processes to Integrate Fraud Risk

Fraud risks can be integrated by leveraging a variety of existing processes. Participants shared that this approach maximizes data sharing between processes owners while minimizing burden in identifying and integrating risks.

General Interviews and Entity-Level Risk Assessments

Participants shared that the ERM process, in particular the risk identification phase, can be leveraged to identify potential areas of fraud. For example, one participant requested input from interviewees on potential areas of weakness and used the input to develop fraud risk statements. Then, the participant rated these statements based on impact, likelihood, and effectiveness of

[22] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/procurement_guides/emergency_acquisitions_guide.pdf

internal controls. Finally, the participant developed a fraud register to track future mitigation activities, if any.

In addition to fraud, practitioners should also consider certain personnel matters, such as misconduct, performance issues, and employee negligence, which may include instances of waste and abuse.

As previously discussed, some participants have conducted "component-level" risk assessments and used the results to inform the OIG Risk Profile with regard to fraud risk (Green Book, Principle 8 (Assess Fraud Risk)). As part of these risk assessments, the individual components considered the potential for internal fraud, waste, and abuse in relation to the following:

- Management components considered purchasing (including change order abuse, conflicts of interest, fictitious vendors, personal and unallowable purchases, and contractor overcharges), travel card use (personal use, delinquent accounts), travel vouchers (personal, excessive, or disallowed travel claims), and IT vulnerabilities (phishing scams, viruses, spyware, data breaches, and external intrusion and hacking).

- Investigation components considered the abuse of authority (improper use of force, negligent discharge of OIG firearms, violations of constitutional rights), criminal activity and serious administrative misconduct by OIG personnel (workers' compensation fraud, computer misuse), the failure to properly obtain or store evidence, the loss or theft of OIG firearms law enforcement credentials or equipment, the misuse of a Government Owned Vehicle, and insider threats.

- Audit components considered independence violations, lack of controls to monitor required communications with stakeholders (Congress, department, agency, and public), and OIG non-conformance with GAO Yellow Book standards and guidance.

Leveraging Quality Assurance Reviews

To integrate ERM within the organizational culture, participants have also begun to embed the assessment of fraud risk within their QAR activities. Specifically, internal QAR groups have employed a number of proactive steps to consider the potential for fraud risk, including:

- cross-functional review teams for added independence and insights (to include the use of external SMEs from other OIGs via reimbursable agreements);

- Program Review Checklists with specific fraud risk assessment steps;

- interviews of applicable managers, employees, and customers to assess concerns or perspectives relative to fraud risk in the program or process under review;

- reviews of position descriptions, directives, systems, and processes to ensure appropriate access levels and adequate separation of duties;

- unannounced reviews of financial accounts (e.g., a confidential funds account) to ensure accountability of funds; and

- physical inventory of sensitive and controlled items in OIG custody (e.g., cash evidence, contraband, firearms, ammunition, etc.).

Following the implementation of ERM, one practitioner reviewed QAR reports that the internal QAR group issued to identify risks, including fraud risks, or factors that could affect the risk of fraud. The QAR group now considers the component-level risk assessment results and the OIG Risk Profile to formulate its Annual QAR Work Plan and to help plan individual QAR projects. The group members continue to consider results of their QARs continue during annual OIG Risk Profile updates. In this way, ERM and quality assurance are integrated.

Moreover, the QAR group considers relevant fraud risks during the planning stages of each QAR. For instance, their Computer Assisted Audit Techniques (CAAT) Team developed a Purchase Card Data Analysis Tool, which the group uses to generate reports about potentially questionable OIG purchase card transactions such as purchases associated with questionable MCC codes (Merchant Category Codes) or possible split transactions. The group uses these reports to help select a sample that targets purchase transactions associated with fraud indicators for testing.

Leveraging Internal Affairs Investigations

Many OIGs have a group chartered to perform Internal Affairs (IA) investigations into allegations of OIG employee misconduct. While such IA cases are sensitive and highly controlled, they can help flag areas or topics for potential risk of fraud, waste, or abuse related to employee misconduct. Regardless of the OIG's structure, IA groups should ensure that their relevant investigative results, along with any identified fraud risks, are considered during ERM activities (as necessary) without disclosing sensitive information.

Leveraging Strategic Planning

Strategic plans are governed by GPRAMA, which requires Federal entities to publish 4-year strategic plans the first Monday following a presidential term. Some participants involved in the strategic planning process at their OIG organizations have placed emphasis on meeting the expectations set forth in GPRAMA, the CIGIE Silver Book, and OMB Circular A-11, part 6, including the following principles:

- setting clear, ambitious goals for outcome-focused and management priorities;

- measuring, analyzing, and communicating performance information to identify successful practices to spread and to identify problematic practices to prevent or correct;

- conducting in-depth performance reviews to drive progress on their priorities;

- engaging leadership in setting goals that reflect priorities, conducting frequent data driven reviews, and communicating results to solve problems and improve outcomes; and

- aligning personnel performance to organizational results.

The strategic plan presents the general and long-term goals an OIG aims to achieve, including the actions OIG will take to realize those goals, and how the agency will address challenges and risks that may impede implementation. Incorporation of ERM into the initial stages of the strategic planning process helps to ensure that an agency's overall mission, objectives, and priorities are realistically aligned with risk appetite. By identifying the close relationship between ERM and strategic planning in the planning process, some participants were able to build greater synergy in both areas simultaneously.

For example, during the initial stages of ERM development, one participant conducted a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis exercise with leadership and staff to help identify risks and opportunities. The resultant data was intended for use in development of the agency risk profile. However, during the initial drafting of the strategic plan, the SWOT information collected was used in a different manner than originally intended. The results provided leadership with a greater understanding of fundamental agency challenges and potential strategic implications, and informed the development of strategic goals and objectives. This participant experienced significant leadership resistance to implement a traditional ERM program. However, by leveraging strategic planning, the participant was able to initiate risk-based practices and discussions. In doing so, the agency published a strategic plan (see Figure 7) and developed a strategic implementation process geared towards operationalizing the strategy while considering risks. Without using traditional ERM language and terms, the participant identified and then cataloged risks to and from its strategic plan. In addition, the agency identified risks to the overall enterprise, furthering its efforts toward full ERM implementation.

Strategic planning represents an opportunity for ERM to add value to agencies through greater awareness of agency risk and posture when setting goals and objectives and mapping out a realistic approach to mission achievement. Although implementing ERM through strategic planning is not the traditional approach using standard ERM methodologies, it may be an option for organizations that are facing difficulties with customary implementation.

Participants leverage the strategic plan to cascade multiyear goals into risk-informed objectives. The objectives are then further refined by developing yearly performance indicators and targets informed by their risk inventory and priority areas.

Figure 7: Sample OIG 2018–2022 Strategic Plan Goals and Objectives

Leveraging Performance Management

Performance management enables Federal agencies to address and improve accountability to taxpayers by setting performance targets and measuring effectiveness.

ERM supports performance management by enabling agencies to anticipate risk and by providing a greater understanding of the impact of risk on performance. By aligning risk appetite and strategy when developing performance indicators, agencies can improve effectiveness and reduce performance variability (risk tolerance). By having an understanding of the tolerance for variation

in performance, management can effectively enhance value for the organization and promote accountability. Operating within defined tolerance provides management with greater confidence that the organization remains within its risk appetite and provides a higher degree of comfort that the organization will achieve its strategic goals and objectives (COSO 2017).

Participants shared that by understanding potential risks against the organization's strategic goals and objectives, response activities and opportunities can be fully integrated with performance. Performance measures can include activities to mitigate risks against core processes, internal controls, and strategic objectives. As depicted in Figure 8, governance bodies, such as the RMC, can provide ongoing dialogue and accountability as they relate to the achievement of strategic goals and objectives.

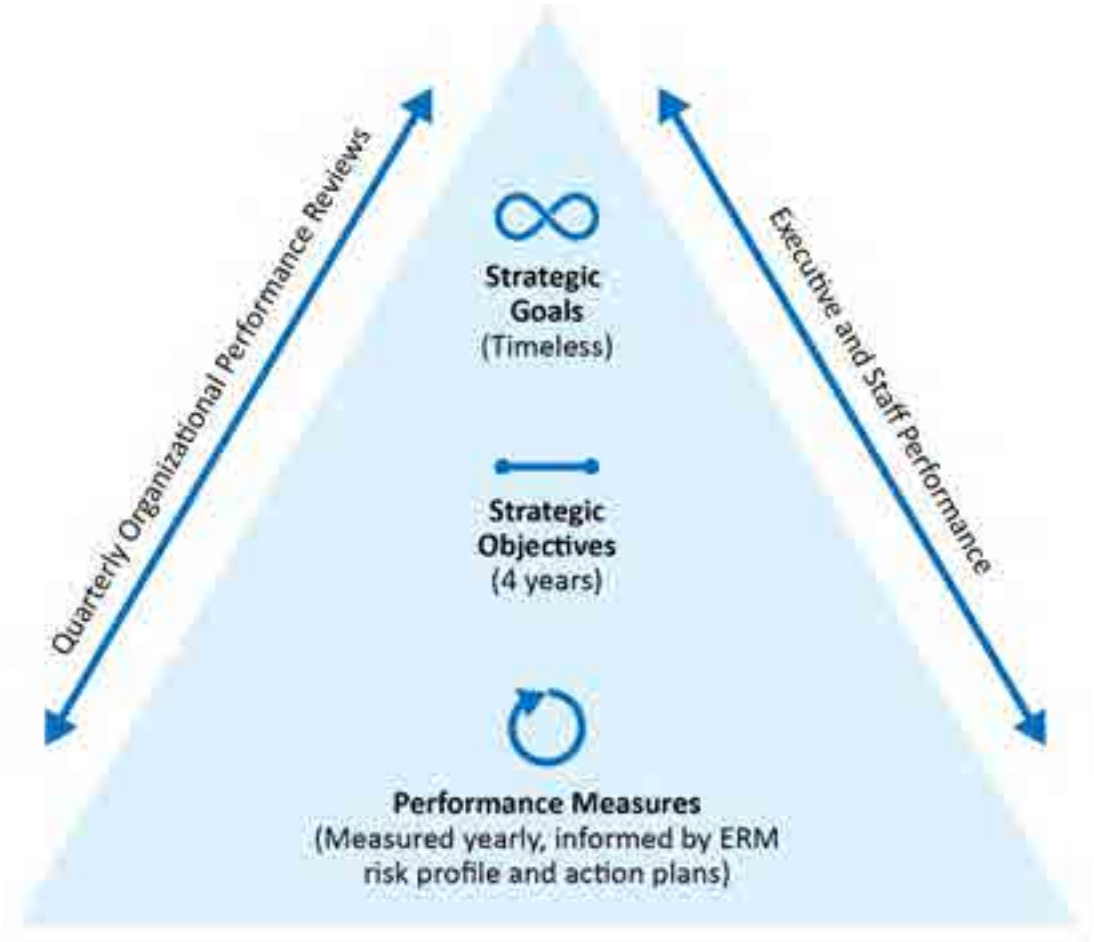
Figure 8: Integrating ERM to Optimize Organizational Performance

ERM, strategic planning, and performance are different activities that, when carefully connected, can optimize governmental effectiveness. Some participants stated that following the publishing of their strategic plans, they worked with executives to develop performance measures that supported such strategic plans. These performance measures were derived from the risk profiles as well as leadership's action plans (activities determined to be priority by leadership). Performance measures were then integrated in both executive and staff annual performance plans to reinforce accountability. One working group participant shared that her OIG organization instituted QPRs to monitor progress related to performance measures.

QPRs are used to measure executive and staff performance and the outcome of the QPRs would be to establish strategic goals and objectives. QPRs should be executed and measured annually. During the QPRs, executives discussed accomplishments, risks, challenges, and corrective action plans. The goal was to monitor performance throughout the year to avoid surprises and to promote collaboration and exchange of ideas among executives.

As depicted in Figure 9, a QPR, coupled with RMC sessions to monitor action plans, represents a holistic governance structure to integrate both performance and risk management.

Figure 9: Strategy & Performance Framework



SUSTAINING ERM

To sustain ERM means to strengthen and obtain support for the implementation and execution of the program or process over time. Furthermore, the ERM process evolution refers to improvements made to ERM as part of facilitating program advancement. ERM requires constant attention and adjustment to be effectively sustained over time. Although all working group participants strive to maintain a sustained ERM process at their respective OIGs, none of them is content with where their programs stand to date. Instead, participants have plans to mature and enhance their ERM programs by adding new components, eliminating ineffective elements, and implementing technological upgrades. Sustaining ERM is an important element in the execution and maintenance process because it allows for evolution and further advancements to occur.

Sustaining an effective ERM environment is different for every organization. ERM environments are formed on the foundation of the organization's culture. Because culture is unique to the organization, the ERM environment is unique as well. Although there is some uniqueness among OIGs, working group participants from organizations with more mature ERM programs within the OIG community agreed that sustaining an effective ERM culture must be accomplished through a blend of the push and pull approaches. The push approach is commonly used for risk monitoring and the pull approach is used for risk assessment.

Evaluation of the ERM program is vital for it to be sustained in the short and long term. When reporting to the audit arm of OIG, practitioners should possess the objectivity and good judgment to examine, evaluate, report, and recommend improvements on the adequacy and effectiveness of management's ERM program.

Building Capabilities

Public sector organizations around the world often must manage and survive volatility, complexity, and ambiguity. Although risk management is not a new concept, ERM is relatively new to the Federal Government. ERM was introduced to the Federal Government a little over a decade ago. However, when OMB Circular A-123 was published in 2016, a broader group of government organizations began seeking ways to introduce ERM into the workforce. With any new initiative, capability building is a necessity. Participants shared three capability-building recommendations: (1) training, (2) subscription services and outside vendors, and (3) crowdsourcing.

Participants manage most OIG ERM programs in small teams. OIG organizations with a robust ERM program are not only advancing their capabilities, but they are also integrating risk management into other activities such as strategic planning, performance management, and audit planning. With limited resources for such a major program, some OIG organizations have identified ERM liaisons and volunteers to help execute and sustain their programs. Because most ERM liaisons and volunteers are not skilled in risk management or ERM, organizations have invested resources to building their capabilities. However, some OIG organizations do not have the luxury of investing resources because they have only a team of one to manage ERM and coordinate with senior management. Even leadership and senior management require some level

of familiarization with the ERM process and its value for the program to be successful and sustained over time.

Training

Organizations have instituted a number of initiatives to train the workforce in ERM. Participants familiarized their workforce with ERM through in-house training sessions and presentations, as well as classes given by training providers. Others engaged in ERM certificate training through various organizations. Nonetheless, most organizations build capabilities through internal educational opportunities, such as town hall meetings, blogs, professional networking, newsletters and conference attendance.

Participants rotate their ERM team members on an annual basis to ensure that members have direct exposure to the process. Members are notified of available training, and those who attend are asked to return to the office and share what they learned with the community. The ERM team itself provides presentations to all OIG staff, including ERM updates, current priority risks, and how ERM impacts them and their daily work.

Subscription Services and Outside Vendors

Subscription services and outside vendors can be useful in building ERM capabilities within an organization. Few participants acquired risk management subscription services to attain access to templates, benchmarking information, assessments, and training or to support implementing ERM. In addition, when acquiring an ERM subscription, all employees across the organization have access to risk-related resources, industry best practices, survey results, and webinars.

Participants indicated that they leveraged outside vendors to train staff on ERM. While the classes are not mandatory, it is very helpful for staff to immerse themselves in the risk culture and ERM concepts. In addition, some participants facilitated a risk community of interest, established to share good practices and aid in building capabilities not only for practitioners but also for the entire organization. Participation in the risk community is optional, and all are welcome to attend.

Crowdsourcing

Crowdsourcing is a practice used to obtain information or input for a task or project by reaching out to people from various levels. Some participants are engaging in this concept by surveying and interviewing top executives to determine what is of greatest risk to the enterprise and simultaneously enlisting feedback from staff at lower levels. In doing so, the ERM team is able to identify emerging risks that may be positioned in executive "blind spots." Not all risks rise to the enterprise level; therefore, internal discussions must occur on how components can maintain their own risk registers and elevate risks to the enterprise level, as appropriate.

Participants also leverage a large-scale online risk assessment survey that involves seeking anonymous input from all staff at the GS-14 level and above (approximately 120 staff members). The survey involves rating the degree of impact and likelihood of occurrence for a number of

enterprise-level risks facing the OIG organization, determining the effectiveness of existing mitigation strategies, and prioritizing the risks on which to focus substantial attention. By enabling wide participation, the survey will promote engagement, as well as capture staff's knowledge and insight in a variety of risk areas.

Automation Resources

Most participants started their ERM efforts by leveraging Excel spreadsheets to identify, analyze, and monitor risks. Often information is conveyed in Word, MS Project, and PowerPoint. Some are maturing their approach to automation by undertaking a project that would integrate performance and risk management in a commercial-off-the-shelf (COTS) enterprise platform. One participant reprogrammed an automated tracking system for time and productivity to capture the risk assessments of audit recommendations based on ERM. The database is used to produce dashboards to monitor high-risk unimplemented recommendations, identify high-risk areas to conduct follow-up audits, and identify emerging high-risk program areas warranting an audit.

This new approach of automating ERM efforts would improve an agency's ability to identify, analyze, and monitor risk mitigation activities, as well as monitor, measure, and report organizational performance against meeting strategic goals.

Although current market research demonstrates that plenty of software is available to support ERM, the focus of any automation effort should be to enable a continual process of obtaining, monitoring, promoting accountability, and sharing information across the organization.

Maturity Model

Once an organization decides to develop and implement ERM, the first step includes assessing its level of maturity. The primary reason for assessing the maturity level of the ERM framework is to ensure that OIG management has a comprehensive understanding of its capabilities to manage risks to the desired level on a consistent, sustainable basis. The capabilities to manage risk include strategies, processes, people, technology, and information. The maturity level can be expressed in several diverse ways. Participants used the Risk Management Society's (RIMS™) Risk Maturity Model to assess maturity levels on an ongoing basis. The goal is to reach the highest level of organizational maturity in which risk procedures are communicated and fully understood throughout the organization and risk management principles are integrated fully within the management process. The maturity levels for the RIMS™ model include ad hoc, initial, repeatable, managed, and leadership.

Other maturity models that can be used to define an organization's level of maturity include the following examples:

- very immature, developing, evolving, mature, and robust;
- nascent, emerging, integrated, predictive, and advanced;
- ad hoc, repeatable, defined, managed, and optimized; and
- ad hoc, initial, repeatable, managed, and leadership.

It is expected that OIG organizations with ERM programs in place may incrementally advance in their maturity levels over the years. As such, it is advisable to complete the maturity assessments yearly to determine progress. (See Exhibit B for details.)

ERM maturity assessment models are widely available at no cost online. There are also paid services that can conduct benchmarking maturity assessments and diagnostic tools. By understanding an organization's ERM maturity level, we can identify areas of strengths and opportunities, identify weak links that inhibit further performance, and plan priorities. All participants have taken a free ERM maturity assessment sometime in the past and have determined their OIG's organizational maturity to be at level 1 (Ad Hoc) or 2 (initial), with aspirations to graduate to level 3 (repeatable) within the next 3 years or so. Some of them conduct these assessments every year.

Participants conduct yearly after-action discussions to pinpoint areas of improvement and plan future process enhancements. They also plan to conduct external assessments (conducted by another OIG organization) to independently determine adherence to OMB Circular A-123 and other best practices.

One sign of ERM maturity is an organization's standardized processes and documented procedures. To this end, OIG organizations are taking steps to document and institutionalize ERM in several ways. A few participants are linking risk mitigation action plans to executive and staff performance plans. Some OIGs are seeking to develop Inspector General Directives to formalize their ERM approaches. Others plan to conduct recurring quality assurance reviews.

Identifying and Improving Risk Culture

Risk culture is a term describing the values, beliefs, knowledge, attitudes, and understanding about risks shared by a group of people with a common purpose.[23] To have an effective risk management program, an organization should cultivate and maintain a strong risk culture anchored on employee engagement. As the OIG community continues to develop and mature its risk management capabilities and programs, it should also work towards cultivating a culture of engagement where risks can be openly communicated and discussed.

No matter how good an organization's risk infrastructure is, risk management is essentially a people issue. Organizations can enable the development of a mature risk culture in which people within the organization take responsibility for identifying and managing risk. To enable a risk culture, participants leverage different approaches to understand and improve their organizational culture.

Participants conduct yearly in-depth analyses of both the FEVS and the Partnership for Public Service's Best Places to Work annual results. The information derived from the analysis provides key insights regarding employee perspectives on engagement, leadership, innovation, fairness, strategic management, and many other issues. Based on trends, the organization develops targeted action plans to improve employee engagement and, subsequently, risk culture.

[23] The Institute of Risk Management (www.theirm.org)

Participants use risk culture surveys to understand respondents' perception of the organization's risk awareness, leaders' risk behaviors, and capabilities. The data from these surveys enables the organization to understand the state of its risk culture, analytics of cultural trends, and lessons learned analysis that can be used to improve ERM activities. Risk survey culture elements and questions[24] leveraged by one participant included the following:

1. Leadership Behaviors:
    a. Leaders in my organization demonstrate risk-awareness behaviors.
    b. Decision makers reach balance between avoiding risks and pursuing opportunities.

2. Personal Risk Awareness:
    a. I understand the organization's risk appetite.
    b. I know the steps I can take to help manage risks in my work.

3. Risk Management Capacity:
    a. The organization provides effective risk management training.
    b. I can learn from my peers when it comes to good risk management behaviors.

The scale used for risk culture surveys can vary, but the range should allow survey participants to indicate their level of agreement including strongly agree, neither agree nor disagree, and strongly disagree.

A similar approach includes improving risk culture from the top down. A participant collaborates with the human resources team to identify and distribute a risk culture survey to all supervisory employees annually (mostly GS 13s and above). Specifically, the survey aims to enhance self-awareness and improve the risk culture within leadership and management then cascade down to the lower levels of the organization.

[24] Gartner, Inc., "Enterprise Risk Assessment Tool"

EXHIBIT A: APPLICABLE LAWS AND POLICIES

ERM-Related Federal Requirements
OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf
OMB Circular No. A-11, part 6, "Strategic Plans, Annual Performance Plans, Performance Reviews, and Annual Program Performance Reports," June 2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf
Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Federal Offices of Inspector General* (Silver Book), August 2012. https://www.ignet.gov/sites/default/files/files/Silver%20Book%20Revision%20-%208-20-12r.pdf
Government Accountability Office *Standards for Internal Control in the Federal Government* (Green Book), September 2014. https://www.gao.gov/assets/670/665712.pdf
Public Law 114-186, *Fraud Reduction and Data Analytics Act of 2015*, June 30, 2016. https://congress.gov/114/plaws/publ186/PLAW-114publ186.pdf
GAO-15-593SP, *A Framework for Managing Fraud Risks in Federal Programs*, July 2015. https://www.gao.gov/assets/680/671664.pdf

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016

(https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf)

OMB Circular A-123 requires agencies to implement an ERM capability coordinated with the strategic planning and strategic review process established by the *Government Performance and Results Act Modernization Act* and the internal control processes required by the *Federal Managers' Financial Integrity Act* and the Government Accountability Office's *Standards for Internal Control in the Federal Government*.

Federal leaders and managers are responsible for establishing goals and objectives around operating environments, ensuring compliance with relevant laws and regulations, and managing both expected and unexpected or unanticipated events. They are responsible for implementing management practices that identify, assess, respond to, and report on risks. Annually, agencies must develop a risk profile coordinated with their annual strategic reviews. OMB Circular A-123 requires agencies to integrate risk management and internal control functions.

OMB Circular A-123 provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by identifying and

managing risks, establishing requirements to assess, correct, and report on the effectiveness of internal controls.

Enterprise Risk Management in Management Practices

Risk management is a series of coordinated activities to direct and control challenges or threats to achieving an organization's goals and objectives. ERM is an effective agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery. While agencies cannot respond to all risks related to achieving strategic objectives and performance goals, they must identify, measure, and assess risks related to mission delivery. Effective risk management:

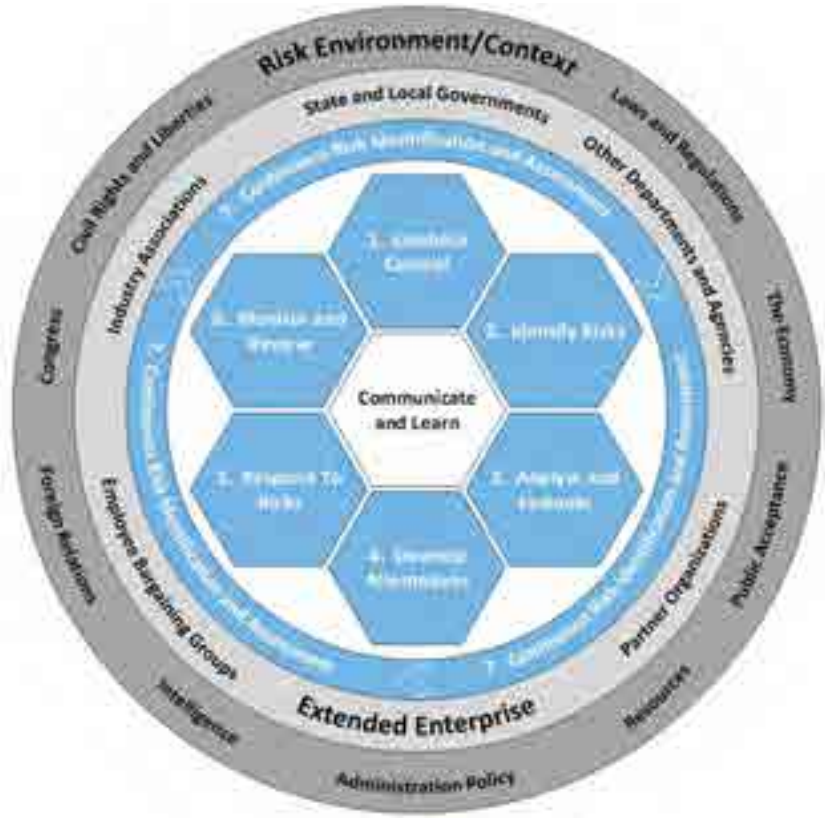
- creates and protects value;
- is an integral part of all organizational processes;
- is part of decision-making;
- explicitly addresses uncertainty;
- is systematic, structured, and timely;
- is based on the best available information;
- is tailored and responsive to the evolving risk profile of the agency;
- takes human and cultural factors into account;
- is transparent and inclusive;
- is dynamic, iterative, and responsive to change; and
- facilitates continual improvement of the organization.

ERM reflects forward-looking management decisions and balancing risks and returns so an agency enhances its value to the taxpayer and increases its ability to achieve its strategic objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM framework also includes the concepts of risk appetite, risk tolerance, and portfolio view.

- Risk appetite is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision.
- Risk tolerance is the acceptable level of variance in performance relative to the achievement of objectives.
- A portfolio view of risk provides insight into all areas of organizational exposure to risk, 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 is beneficial because it addresses a fundamental organizational issue: the need for information about major risks to flow both up and down the organization and across its organizational structures to improve the quality of decision-making. Although there are many approaches that can be taken to implement ERM, most include the following elements (Figure 10):

Figure 10: Example of an Enterprise Risk Management Model



1. Establish the Context: understanding and articulating the internal and external environments of the organization.
2. Initial Risk Identification: using a structured and systematic approach to recognizing where the potential for undesired outcomes or opportunities can arise.
3. Analyze and Evaluate Risks: considering the causes, sources, probability of the risk occurring, the potential positive or negative outcomes, and then prioritizing the results of the analysis.
4. Develop Alternatives: systematically identifying and assessing a range of risk response options guided by risk appetite.
5. Respond to Risks: making decisions about the best options(s) among a number of alternatives, and then preparing and executing the selected response strategy.
6. Monitor and Review: evaluating and monitoring performance to determine whether the implemented risk management options achieved the stated goals and objectives.
7. Continuous Risk Identification: must be an iterative process, occurring throughout the year to include surveillance of leading indicators of future risk from internal and external environments.

The "extended enterprise" consists of interdependent relationships, parent-child relationships, and relationships external to an agency. Thus, no agency is self-contained, and risk drivers can arise out of organizations that extend beyond the enterprise. These relationships give rise to a need for assurance that risk is being managed in that relationship both appropriately and as

planned. The risk environment is beyond the boundary of the "extended enterprise." The environment generates risks that cannot be controlled or constrains the way the organization is permitted to take on or address risk.

A. Governance

To provide governance for the risk management function, agencies may use a Risk Management Council (RMC) to oversee the establishment of the agency's risk profile, regular assessment of risk, and development of appropriate risk response options. An effective RMC will include senior officials for program operations and mission-support functions to help ensure those risks are identified which have the most significant impact on the mission outcomes of the agency. Should agencies choose to use an RMC, the agency's Chief Operating Officer or a senior official with responsibility for the enterprise should chair the RMC. Agency governance should include a process for considering risk appetite and tolerance levels. The concept of "risk appetite" is key to achieving effective ERM and is essential to consider in determining risk responses.

B. Risk Profiles

Agencies must maintain a risk profile. The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an agency faces to achieve its strategic objectives arising from its activities and operations and to identify appropriate options for addressing significant risks. The risk profile is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process, instead of a complete inventory of risks. Agencies have discretion in terms of the appropriate content and format for their risk profiles; however, in general, risk profiles should include the following seven components:

1. Identification of Objectives
2. Identification of Risk
3. Inherent Risk Assessment
4. Current Risk Response
5. Residual Risk Assessment
6. Proposed Risk Response
7. Proposed Action Category

OMB Circular A-11, Part 6, "Strategic Plans, Annual Performance Plans, Performance Reviews, and Annual Program Performance Reports," June 2018

(https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf)

OMB Circular A-11, part 6, focuses on performance and strategic reviews, which include agency requirements, guidance on ERM, performance and strategic reviews, and leveraging strategic reviews with ERM. The guidance requires:

- All agencies to implement an ERM capability using guidance found in OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, as appropriate for the agency mission and in accordance with agency-specific programs.

- Agencies to assess and manage risk as a part of a strategic and data-driven review in support of the broader organizational risk management framework, as appropriate for their missions and in accordance with OMB Circular A-123. Guidance found in part 6, sections 270.26–270.29 complements OMB Circular A-123. Agencies should refer to OMB Circular A-123 for a complete description of ERM responsibilities in the Federal Government.

- Agencies to support the identification, assessment, and prioritization of probable risks that may impact program delivery or outcomes and are likely to impact strategic objectives, by coordinating ERM efforts with strategic reviews.

- Agencies to manage risks and challenges related to delivering their organizations' missions. ERM is a strategic discipline that can help agencies to properly identify and manage risks to performance, especially those risks related to achieving strategic objectives. An organizational view of risk positions allows the agency to quickly gauge which risks are directly aligned to achieving strategic objectives, and which have the highest probability of impacting mission. When significant, prioritized risks are vetted and escalated appropriately, challenges and opportunities can be routinely analyzed and incorporated into performance plans. When well executed, ERM improves agency capacity to prioritize efforts, optimize resources, and assess changes in the environment. Instituting ERM can help agency leaders make risk-aware decisions that impact prioritization, performance, and resource allocation.

- The agency's strategic review is a process by which the agency should coordinate its analysis of risk using ERM to make risk-aware decisions, including the development of risk profiles as a component of the annual strategic review; identifying risks arising from mission and mission-support operations; and providing a thoughtful analysis of the risks an agency faces towards achieving its strategic objectives to develop responses that may be used to inform decision-making through existing management processes. The results of the agency's risk assessment in the risk profile should be discussed each year with OMB as a component of the Summary of Findings from the agency strategic review and used to inform agency strategic and performance planning efforts.

- Enterprise risk managers, who may be referred to as the CRO in some agencies, to champion agency-wide efforts to manage risk within the agency and advise senior leaders on the strategically aligned portfolio view of risks at the agency. The responsibilities of managing risk, however, are shared throughout the agency from the highest levels of executive leadership to the service delivery staff executing Federal programs. Agencies are required to have an ERM function and are expected to manage risks to mission, goals, and objectives of the agency.

OMB provides agencies with guidance related to risk management in some specialized areas. Among this guidance are the following:

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016;
- Memorandum -07-24, *Updated Principles for Risk Analysis*, September 19, 2007;

- OMB Circular No. A-129, *Policies for Federal Credit Programs and Non-Tax Receivables*, January 2013; and
- Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 19, 2017.

Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Federal Offices of Inspector General* (Silver Book), August 2012

(https://www.ignet.gov/sites/default/files/files/Silver%20Book%20Revision%20-%208-20-12r.pdf)

Ensuring Internal Control

Efficient and Effective Operations

Each OIG should manage available resources at the least cost to produce the greatest results in terms of public benefit, return on investment, and risk reduction.

Risk Assessment

The Inspector General 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. Risk assessment methodologies and the formality of their documentation may vary from OIG to OIG, depending on the OIG's size, mission, and other factors.

Planning and Coordinating

Each OIG shall maintain a planning system assessing the nature, scope, and inherent risks of agency programs and operations. This assessment forms the basis for establishing strategic and performance plans, including goals, objectives, and performance measures to be accomplished by the OIG within a specific period.

Government Accountability Office, *Standards for Internal Control in the Federal Government* (Green Book), September 2014

(https://www.gao.gov/assets/670/665712.pdf)

Internal Control

Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.

Establishing an Effective Internal Control System

The Green Book defines the standards for internal control in the Federal Government. The *Federal Managers' Financial Integrity Act* requires Federal executive branch entities to establish internal control in accordance with these standards.

The five components of internal control are control environment; risk assessment; control activities; information and communication; and monitoring. Risk assessment assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. The five components are based on 17 principles of internal control. The four principles that apply to risk assessment are discussed in the following paragraphs.

Risk Assessment

Having established an effective control environment, management assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. Management assesses the risks the entity faces from both external and internal sources. Risk assessment is based on the following four principles of internal control:

Principle 6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

6.02 Management defines objectives in specific and measurable terms to enable the design of internal control for related risks.

6.03 Management defines objectives in alignment with the organization's mission, strategic plan, and performance goals.

6.05 Management sets internal expectations and requirements through the established standards of conduct, oversight structure, organizational structure, and expectations of competence as part of the control environment.

6.06 Management evaluates and, if necessary, revises defined objectives so that they are consistent with these requirements and expectations. This consistency enables management to identify and analyze risks associated with achieving the defined objectives.

6.08 Management defines risk tolerances for the defined objectives. Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives.

Principle 7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

7.02 Management identifies risks throughout the entity to provide a basis for analyzing risks. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.

7.03 To identify risks, management considers the types of risks that impact the entity. This includes both inherent and residual risk. Management's lack of response to either risk could cause deficiencies in the internal control system.

7.04 Management considers all significant interactions within the entity and with external parties, changes within the entity's internal and external environment, and other internal and external factors to identify risks throughout the entity. Internal risk factors may include the complex nature of an entity's programs, its organizational structure, or the use of new technology in operational processes. External risk factors may include new or amended laws, regulations, or professional standards; economic instability; or potential natural disasters. Management considers these factors at both the entity and transaction levels to comprehensively identify risks that affect defined objectives. Risk identification methods may include qualitative and quantitative ranking activities, forecasting and strategic planning, and consideration of deficiencies identified through audits and other assessments.

7.05 Management analyzes the identified risks to estimate their significance, which provides a basis for responding to the risks. Significance refers to the effect on achieving a defined objective.

7.06 Management estimates the significance of the identified risks to assess their effect on achieving the defined objectives at both the entity and transaction levels. Management estimates the significance of a risk by considering the magnitude of impact, likelihood of occurrence, and nature of the risk.

7.08 Management designs responses to the analyzed risks so that risks are within the defined risk tolerance for the defined objective. Management designs overall risk responses for the analyzed risks based on the significance of the risk and defined risk tolerance. These risk responses may include acceptance, avoidance, mitigation, reduction, or sharing.

7.09 Based on the selected risk response options, management designs the specific actions to respond to the analyzed risks.

Principle 8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

8.02 Management considers the types of fraud that can occur within the entity to provide a basis for identifying fraud risks. Types of fraud are as follows:

- Fraudulent financial reporting—Intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. This could include intentional alteration of accounting records, misrepresentation of transactions, or intentional misapplication of accounting principles.

- Misappropriation of assets—Theft of an entity's assets. This could include theft of property, embezzlement of receipts, or fraudulent payments.
- Corruption—Bribery and other illegal acts.

8.03 In addition to fraud, management considers other forms of misconduct that can occur, such as waste and abuse. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice given the facts and circumstances.

8.04 Management considers fraud risk factors. Fraud risk factors do not necessarily indicate that fraud exists, but they are often present when fraud occurs. Fraud risk factors include the following:

- Incentive/pressure—Management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud.
- Opportunity—Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud.
- Attitude/rationalization—Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

8.05 Management uses the fraud risk factors to identify fraud risks.

8.06 Management analyzes and responds to identified fraud risks so that they are effectively mitigated. Management analyzes the identified fraud risks by estimating their significance, both individually and in the aggregate, to assess their effect on achieving the defined objectives.

8.07 Management designs an overall risk response option and specific actions for responding to fraud risks. It may be possible to reduce or eliminate certain fraud risks by making changes to the entity's activities and processes.

Principle 9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

9.02 As part of risk assessment or a similar process, management identifies changes that could significantly impact the entity's internal control system. Identifying, analyzing, and responding to change is similar to, if not part of, the entity's regular risk assessment process. However, change is discussed separately because it is critical to an effective internal control system and can often be overlooked or inadequately addressed in the normal course of operations.

9.03 Conditions affecting the entity and its environment continually change. Management identifies, on a timely basis, significant changes to internal and external conditions that have already occurred or are expected to occur. Changes in internal conditions include changes to the entity's programs or activities, oversight structure, organizational structure, personnel, and technology. Changes in external conditions include changes in the governmental, economic, technological, legal, regulatory, and physical environments.

9.04 As part of risk assessment or a similar process, management analyzes and responds to identified changes and related risks to maintain an effective internal control system. Changes in conditions affecting the entity and its environment often require changes to the entity's internal control system because existing controls may not be effective for meeting objectives or addressing risks under changed conditions.

9.05 Further, changing conditions often prompt new risks or changes to existing risks that need to be assessed. As part of analyzing and responding to change, management performs a risk assessment to identify, analyze, and respond to any new risks prompted by the changes.

Public Law 114-186, *Fraud Reduction and Data Analytics Act of 2015*, June 30, 2016

(https://www.congress.gov/114/plaws/publ186/PLAW-114publ186.pdf)

The *Fraud Reduction and Data Analytics Act of 2015* ("Act") was enacted to improve Federal agency financial and administrative controls and procedures to assess and mitigate fraud risks and to improve Federal agencies' development and use of data analytics for the purpose of identifying, preventing, and responding to fraud, including improper payments.

Section 3: Establishment of Financial and Administrative Controls Relating to Fraud and Improper Payments

This Act requires the Director of the Office of Management and Budget, in consultation with the Comptroller General of the United States, to establish guidelines for agencies to establish financial and administrative controls to identify and assess fraud risks and design and implement control activities to prevent, detect, and respond to fraud, including improper payments. The guidelines described in section 3 of the Act shall incorporate the leading practices identified in the report published by the Government Accountability Office on July 28, 2015, entitled *Framework for Managing Fraud Risks in Federal Programs*.

Requirements for Controls

Subsection (b) adds that the financial and administrative controls required to be established by agencies shall include—

(1) conducting an evaluation of fraud risks and using a risk-based approach to design and implement financial and administrative control activities to mitigate identified fraud risks;

(2) collecting and analyzing data from reporting mechanisms on detect fraud to monitor fraud trends and using that data and information to continuously improve fraud prevention controls; and

(3) using the results of monitoring, evaluation, audits, and investigations to improve fraud prevention, detection, and response.

GAO-15-593SP, *A Framework for Managing Fraud Risks in Federal Programs*, July 2015

(https://www.gao.gov/assets/680/671664.pdf)

To help managers combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks and organized them into a conceptual framework described in *A Framework for Managing Fraud Risks in the Federal Government* (the [Fraud] Framework). The [Fraud] Framework encompasses control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks. GAO conducted this study to identify leading practices and to conceptualize these practices into a risk-based framework to aid program managers in managing fraud risks.

Managers of government programs maintain the primary responsibility for enhancing program integrity; however, the OMB plays a key role in issuing guidance to assist managers with combating government-wide fraud, waste, and abuse. Legislation and guidance has increasingly focused on the need for program managers to take a strategic approach to managing risks, including fraud. In 2014, OMB recommended that agencies consider adopting enterprise-wide risk management, an approach for addressing the full spectrum of risks and challenges related to achieving the agencies' missions.

GAO's work has shown that opportunities exist for Federal managers to take a strategic, risk-based approach to managing fraud risks and developing effective antifraud controls. Agencies may have existing departments that are responsible for enterprise-wide risk management or managing risks related to improper payments. These departments may have functions that overlap with fraud risk management activities, and they may be able to incorporate the roles and responsibilities of the antifraud entity. An agency may have enterprise-wide or other risk management activities; such as processes to assess risks, that affect operations or compliance with laws. These activities can inform the specific approach taken for assessing fraud risks.

EXHIBIT B: RIMS™ ERM MATURITY LEVELS

Maturity (level)	Maturity (level) Maturity Level Characteristics
Ad hoc (1)	The organization may be compliant with legal and regulatory requirements, but without consistent, formalized or documented risk management arrangements or processes. Implies an extremely primitive level of ERM maturity in which risk management typically depends on the actions of specific individuals, with improvised procedures and poorly understood processes.
Initial (2)	The organization is aware of the need for a more formal risk management approach. Risk management arrangements and processes are structured but incompletely put into practice. Formalization is ongoing but not fully accepted in the organization. Risk is managed independently, with little integration or risk gathering from all parts of the organization. Processes typically lack discipline and rigor. Risk definitions often vary across the organization. Risk is managed in silos, with little integration or risk aggregation. Processes typically lack discipline and rigor. Risk definitions often vary across the silos.
Repeatable (3)	Risk management arrangements and processes are standardized with defined and documented procedures. Risk management awareness may be included in organizational training. A standardized procedure is generally in place with the senior levels of the organization being provided with risk overviews/reports. Risk management is aligned with the organization's external and internal environment, as well as the organization's risk profile. The risk management arrangements and processes are established and repeatable as a standard organizational approach. Risk assessments are conducted throughout departments with the goal of gathering input from the frontline. Information is aggregated to the board of directors, senior management, committees and regulators for risk overviews. Approaches to risk management are established and repeatable.
Managed (4)	Enterprise-wide risk management activities, such as monitoring, measuring, and reporting are integrated and harmonized with measures and controls established. Risk arrangements, assessments, and treatments are organized, monitored, and managed at many levels of the organization. Risk information is structured in a manner that it can easily be cascaded throughout the organization for information collection and aggregated for senior level reporting. Measurement metrics are standardized and incorporated into the organization's performance metrics. Risk procedures are communicated and fully understood throughout the organization with the risk management principles integrated fully within the management process. Mechanisms are in place for alerting management about changes in the organization's risk profile that may affect the organization's objectives.
Leadership (5)	Risk procedures are communicated and fully understood throughout the organization with the risk management principles integrated fully within the management process. Risk-based discussions are embedded to a strategic level, such as long-term planning, capital allocation, and decision-making. Risk appetite (risk/reward) and tolerances are clearly understood with alerts in place to ensure the board of directors and executive management is made aware when set thresholds are exceeded. Planned critical review of the risk management program provides guidance for adjusting/improving application of the risk management principles, arrangements, and processes across the organization to advance objectives.

[25] The Risk Management Society ™

EXHIBIT C: STRATEGIC PLAN EXAMPLES

EXAMPLE #1

Vision

We are a collaborative team of diverse, empowered professionals committed to excellence, innovation, our core values, and sharing our knowledge and best practices with the agency and the Inspector General community. We leverage the specialized skill sets within the Office of Inspector General (OIG) to bring heightened awareness to agency's toughest challenges. We support the agency's efforts to achieve stronger housing markets, quality and safer housing, and strengthened communities.

Mission

We promote economy, efficiency, and effectiveness in the administration of agency programs with traditional and innovative approaches. We protect the integrity of agency programs and operations by identifying opportunities for agency programs to progress and succeed.

Strategic Goals and Objectives

Goal 1: Further the agency's mission success

1.1 Use risk-based approaches to prioritize and plan cross-functional work
1.2 Leverage traditional and innovative approaches to provide high-quality and insightful work products
1.3 Influence the agency's' decision-making through relevant, timely reports that address root causes and identify lasting solutions to issues reported

Goal 2: Advance operational economy, efficiency, and effectiveness

2.1 Evaluate and update practices to ensure mission and mission support work is timely, relevant, impactful, measurable, and transparent
2.2 Ensure organizational structures, staffing, and technological tools support our mission and vision
2.3 Improve long-term planning and visibility in financial management, acquisition, and resource allocation across the organization

Goal 3: Cultivate positive internal and external stakeholder relations

3.1 Use new and existing processes to identify and improve our working relationships with stakeholders to identify emerging risks, better understand their perspectives and needs, and gather their feedback

33.2 Initiate and participate in the Inspector General community and industry coalitions that further our ability to enhance Federal Government performance in service to the taxpayer
3.3 Share fraud and abuse prevention communications with the agency's program participants and employees

Goal 4: Invest in ourselves and our organizational culture

4.1 Attract, develop, empower, and retain a competent workforce
4.2 Promote intra-OIG trust and collaboration by engaging employees at all levels in decision-making, living our core values, and improving communications
4.3 Reinvent our policies and practices for performance management and employee recognition in favor of teamwork and shared accomplishments

Goal 5: Foster strategic thinking and long-term planning

5.1 Model our leadership philosophy and commit to continual process improvement to demonstrate leadership at all levels of the organization
5.2 Facilitate greater outcomes by improving organization-wide engagement and capitalizing on our diverse specialized expertise
5.3 Optimize resource management to support current and future requirements and goals

Core Values

Accountability is taking ownership of our decisions and actions. We hold one another accountable to a higher standard of conduct.

Courage is doing what is right, no matter how difficult. We ask questions and raise concerns when needed.

Respect is appreciating the uniqueness of our workforce. We treat others with dignity, civility, and mutual consideration.

Stewardship is accepting our responsibility to serve the public good. We care about leaving things better than we found them.

Trust is the result of promises kept. We deliver on our commitments and communicate honestly with our stakeholders.

EXAMPLE #2

Achieving Our Mission and Vision

There is risk in not knowing how our mission, vision, strategic goals and objectives may be affected by potential events, such as those prompted by economic, political, and environmental change. The risk of an event occurring creates uncertainty. In this context, risk is defined as the possibility of unplanned or unexpected events occurring that adversely affect the achievement of our strategic and business goals and objectives.

We informed our approach to strategy and performance management by requirements set forth by the *Government Performance and Results Act Modernization Act of 2010*, and OMB Circular A-11, part 6. We continuously use ERM outputs in strategic planning, performance planning, and reporting processes to ensure that our management of risk is aligned with our mission, goal, objectives and priorities.

Our core values of Excellence, Integrity, Independence, Service, and Transparency define how we do our work, and guide our leadership in making decisions that optimize performance and stewardship to achieve mission success.

Our Mission

We serve the American people, the agency, and Congress by providing independent and objective oversight of Departmental programs through audits and investigations and by combatting the influence of labor racketeering in the workplace.

Our Vision

We strive to:

- enhance through our oversight, the ability of the agency to address emerging workforce challenges and
- foster a thriving work environment that values employees as our greatest asset.

Core Values

Our core values of ***Excellence, Integrity, Independence, Service, and Transparency*** guide our leadership in making decisions that optimize performance and stewardship in the current environment. Constant attention to these core values, which are embodied in all of our work, leads to mission success.

Excellence	We deliver relevant, quality, timely, high-impact products and services, through a workforce committed to accountability and the highest professional standards.
Integrity	We adhere to the highest ethical principles and perform our work in an honest and trustworthy manner.
Independence	We are committed to being free of conflicts of interest through objectivity and impartiality.
Service	We are a unified team, vigilant to duty through dedicated public service.
Transparency	We promote an environment of open communication through information sharing, accountability, and accurate reporting.

Strategic Goals and Objectives

Three strategic goals guide our work and focus on ensuring sustainability, accountability, and transparency in our operations.

Our strategic goals are:

Strategic Goal 1	Deliver timely, relevant, and high-impact results.
Strategic Goal 2	Foster an internal OIG culture that drives high performance and engagement.
Strategic Goal 3	Promote responsible stewardship of OIG financial and non-financial resources.

To measure organizational performance, the OIG developed 13 strategic objectives.

Strategic Goal 1

Deliver timely, relevant, and high-impact results	
Strategic Objective	**Description**
1.1	Strengthen the agency's key programs and operations though our work and other deliverables.
1.2	Improve our work processes to drive the timely completion of relevant and impactful audits and investigations.
1.3	Employ a risk-based approach to prioritize and target audits and investigations on areas that provide the greatest impact and address the highest risks.
1.4	Timely articulate to our external stakeholders the relevance, impact, and value of our work in each product.
1.5	Proactively engage our key stakeholders to seek their input for identifying potential audits and investigations.

Strategic Goal 2

Foster an internal OIG culture that drives high performance and engagement	
Strategic Objective	**Description**
2.1	Create a culture of civility, respect, and inclusiveness at all levels by fostering transparency and timely communications.
2.2	Meet current and future OIG mission needs through continuous development and professional growth.
2.3	Enhance OIG human capital by developing and implementing strategic recruitment, succession, and retention plans.
2.4	Increase management and leadership effectiveness, including seeking staff feedback.

Strategic Goal 3

Promote responsible stewardship of OIG financial and non-financial resources	
Strategic Objective	**Description**
3.1	Develop an OIG budget based on strategic mission priorities, areas of risk, operational needs, and cost effectiveness.
3.2	Ensure proper oversight of resources through effective internal controls.
3.3	Improve mission achievement and increase efficiency through technology.
3.4	Enhance the effectiveness, quality, and customer service of mission support activities.

EXHIBIT D: RISK CATEGORIES, DEFINITIONS, AND EXAMPLES

Strategic Risks

Strategic risks include Internal and External risk factors that would prevent accomplishment of OIG's mission, goals and objectives. Strategic risk is a function of the compatibility of an organization's strategic goals, the resources deployed against the goals, and the quality of execution. Strategic risks can be affected by changes in the oversight environment, our perceived reputation, legislative effect, or management practices. When thinking about strategic risks, consider the concept of effectiveness and our ability to demonstrate and measure the effectiveness of our programs.

Strategic Risks Subcategories

Reputational Risks	Government Environment Risks	Political Risks	Management Risks
The risk that the organization's business practices, behaviors, or decisions do not align with OIG's core values, which could adversely impact the confidence and trust of internal or external stakeholders of the OIG. Stakeholders include Congress, OMB, the Department, employees, the public, CIGIE, and others. **Examples:** • Lack of objectivity and integrity in work conducted • Employee misconduct • Unfair treatment of employees • Loss or release of personally identifiable information • Inadequate oversight or execution of major mission activities • Disconnects with stakeholder expectations • Negative or unproductive relationships with Department officials	Risk that the occurrence of a political event(s) will impact the OIG, its mission, processes, or other activities associated with the status quo, or operations. This risk also includes uncertainty arising from the actions or decisions of government bodies or leaders that can result in policy or regulatory changes affecting the OIG, its people, or mission. **Examples:** • Funding availability • Legislative effect and influence • Executive Orders	Risk that the occurrence of a political event(s) will impact the OIG, its mission, processes, or other activities associated with the status quo or operations. This risk also includes uncertainty arising from the actions or decisions of government bodies or leaders that can result in policy or regulatory changes affecting the OIG, its people, or mission. **Examples:** • Funding availability • Legislative effect and influence	Risk that the OIG's management practices will impact its ability to meet mission goals and objectives. **Examples:** • Organizational structure • Decision-making environment • Effectiveness of OIG oversight activities • Responsiveness and adaptability to change • Effectiveness in managing performance against OIG's strategic goals and objectives • Effectiveness in implementing internal controls • "Tone at the top" • Organizational culture • Alignment with organizational risk appetite • Availability and allocation of resources

Operational Risks

Operational risks are risks arising from inadequate or failed internal processes, systems, people, management, or other internal or external events. If they occur, these risks can cause financial loss, loss of competitive position, fines or sanctions, injury or damage to people or property, or affect achieving OIG's mission, goals, or objectives. Risks to the effective and efficient use of OIG resources may be related to administrative and major program operations. When thinking about operational risks, consider a broad range of activities such as litigation, compliance, business processes, business continuity, resource management, and technology.

Operational Risk Categories

Technological Risks

The broad risk associated with advances in technology and impacts to operations.

Examples:

- Lack of IT resources and skills
- Technological advancements or disruptive technologies that render our systems or activities obsolete or inadequate
- New or untried technologies that impact our current investments or activities
- Network/server failures
- Loss of data
- IT security preparedness

Resource Management Risks

The risk to OIG's effectiveness, reliability, or quality of our products and services, due to how the organization manages key business processes.

Examples:

- **People**: Hiring, developing and retaining talent; having sufficient staff with the appropriate skill sets and knowledge; succession planning; having a diverse workforce.
- **Systems and Processes:** Effectiveness and availability of systems, data, process, access to information and support services needed to carry out mission work; effectiveness in following established procedures, such as obtaining required approvals or clearances; ability to execute work as planned or expected; ability to leverage best practices to meet mission requirements; ability to maintain quality standards for all OIG outputs.
- **Contract Management**: Consistency of contractor performance with contract terms and conditions, including performance standards, cost and schedule milestones, and level of satisfaction with deliverables provided.
- **Financial Management:** Effectiveness of financial management processes including sound budget planning and execution activities, including following Federal budgeting requirements, proper execution of congressional appropriations, accuracy in financial reporting and compliance with relevant laws.
- **Policies and Procedures**: The existence of up-to-date written policies and procedures that effectively provide guidance and clarification for critical work or core functions.
- **Physical Assets**: Facilities, equipment or personal property deemed significant enough to track and monitor.

Hazard Risks

The risk that employee or organizational attitudes, conduct, or lack of awareness of hazards could impact the protection of lives and property, and hinder efforts to prevent accidents and incidents. The risk that OIG will experience loss of critical functions caused by natural disasters or hazards.

Examples:

- Insider threats or personal crimes, including vandalism
- Severe weather events
- Pandemics
- Terrorist attacks
- Workplace incidents caused by disgruntled employees or threats to any individual on site, due to an external threat or event
- Utility failure
- Health hazards
- Cybersecurity threats
- Lawsuits
- Improper use of force

Reporting Risks

Risks related to the reliability of the OIG's reporting, including the accuracy and timeliness needed within the organization to support decision-making and performance evaluations, as well as our ability to meet standards, regulations, and stakeholder expectations. When thinking about reporting risks, consider this risk category as a subset of operational risk.

Examples:

- Failure to comply with statutory audit, investigative, and periodic reporting requirements
- Failure to manage audits to completion within required timeframes
- Failure to report accurate information as part of the Statement of Assurance process
- Inadequate or inaccurate financial reporting
- Failure to provide required notifications to stakeholders
- Failure to provide reports, or provide access to data to senior leadership to enable strategic decision-making
- Failure to comply with any OMB reporting requirement
- Failure to comply with any congressional reporting requirement
- Failure to comply with Department of Justice/CIGIE reporting requirements

Compliance Risks

Risk of failing to comply with applicable laws and regulations and failure to detect and report activities that are not compliant with statutory, regulatory, organizational requirements. Failure to stay abreast of changes in Federal regulations. Compliance risks can be caused by a lack of awareness or ignorance of the pertinence of applicable statutes, regulations or code of conduct or other prescribed requirements. When thinking about reporting risks, consider this risk category as a subset of operational risk. Compliance risks can result in reputational risks.

Examples:

- Failure to comply with laws and regulations pertaining to human capital, IT, financial, procurement, privacy statutes, and regulatory requirements
- Failure to comply with CIGIE audits, investigative, and operational standards
- Failure to comply with professional standards
- Failure to assess OIG performance by evaluating actual to planned performance
- Failure to report a conflict of interest
- Failure to comply with personally identifiable information, records management, or Freedom of Information Act requirements

EXHIBIT E: OTHER RISKS TO CONSIDER

Risk	Definition
Strategic	
Economy	Significant economic changes, in particular an economic downturn, may result in tightening budgets, a smaller workforce
Political Change	Changes in political administrations may shift objectives and focus on different issues.
Operations	
Stakeholder Satisfaction	Inability to provide services or perform certain activities that meet or exceed stakeholder expectations may result in bad press or congressional hearings.
Policies and Procedures	Lack of compliance with established policies and procedures may result in unacceptable performance by employees, which may result in not achieving objectives.
Legal and Regulatory	Failure to comply with laws and regulations may result in legal claims or damage to the organization's reputation.
Human Resources	Failure to effectively attract, develop, and retain qualified people may hinder its ability to execute, manage, and monitor key activities.
Authority	Failure to adequately define and articulate authority levels may result in employees committing the organization to transactions outside of expectations, or confusion on who can commit to what, causing delays or errors in executing necessary transactions.
Integrity	Act committed by employees that are considered unethical, fraudulent, or otherwise inappropriate may result in an inability to conduct operations in accordance with management's expectations.
Leadership/Empowerment	Failure of senior management to provide the necessary direction and leadership, and appropriately empower employees, may result in confusion regarding management's expectations and difficulty in executing the organization's strategic objectives.
Communications	Lack of clear and comprehensive communication up, down, and laterally within the organization may result in misunderstanding regarding management's expectations and untimely identification of performance shortfalls.
Culture	Failure to establish and maintain a culture that promotes behavior consistent with values and expectations may impair the organization's ability to achieve its objectives.
Knowledge Capital	Failure to recognize, exploit, and protect the knowledge capital embedded in the organization's services and employees may result in an inability to achieve strategic objectives.

Risk – cont'd	Definition – cont'd
Outsourcing/Shared Services	Failure to effectively manage and monitor outsourcing arrangements may result in vendor performance that falls short of expectations.
Health and Safety	Failure to protect the health and safety of employees and third parties on organizational property may result in claims, low morale, or reduced productivity.
Finance	
Budget	Inability to prepare meaningful budgets and forecasts may diminish the organization's ability to monitor and understand actual financial and operational results, which could limit the ability to react to performance gaps and modify objectives and performance targets on a timely basis.
Cash Flow	Inability to effectively manage cash outflows may inhibit the organization's ability to meet its obligations.
Accounting	Lack of an effective and efficient account process may result in untimely or inaccurate compilation and reporting of information needed for financial analysis, external reporting of financial results, or internal analysis of operating results.
Information	
Data Integrity	Inability to ensure the integrity of data relied upon for decision-making may result in poor management decisions.
Data Relevance	The existence of irrelevant or unnecessary data in applications or reports may result in inappropriate judgments and decisions.
Systems Infrastructure	Lack of an effective information technology infrastructure (e.g., hardware, networks, software, monitoring tools) may diminish the organization's ability to support the current and future information needs in an efficient and effective manner.
Systems Access	Failure to appropriately restrict access to data or programs may result in unauthorized changes to date or programs, inappropriate access to restricted or confidential information, or inefficiencies where access is too restrictive.
Systems Availability	Systems or data that are not available to the right people at the right time may result in inefficient or ineffective operation of critical processes.

(Sobel 2015)

EXHIBIT F: GLOSSARY

A-123: Refers to OMB Circular A-123, which defines management's responsibility for enterprise risk management and internal control in Federal agencies.

A-123, Appendix A: Refers to OMB Circular A-123, Appendix A (updated in 2018), which defines the management of reporting and data integrity risk.

Acceptance: Risk response where no action is taken to respond to the risk based on the insignificance of the risk, or the risk is knowingly assumed to seize an opportunity.

Acquisition Risk: Risks associated with research, development, testing & evaluation (RDT&E) and procurement of new technologies or technological upgrades of existing systems. Risk responses may include sharing or transferring risk through joint ventures or outsourcing. Innovation should be considered an opportunity space as a failure to innovate may result in future challenges risk.

Avoidance: Risk response in which action is taken to stop the operational process or the part of the operational process causing the risk.

Aggregated Risks: Consideration of risks in combination.

Assess: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Controls: A policy or procedure implemented to reduce the likelihood or consequence of an adverse risk event.

Control Activities: The policies and procedures that help ensure management directives are effectively carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

Compliance Risk: Risk of failing to comply with applicable laws and regulations and the risk of failing to detect and report activities that are not compliant with statutory, regulatory, or organizational requirements. Compliance risk can be caused by a lack of awareness or ignorance of the pertinence of applicable statutes and regulations to operations and practices.

COSO: Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. COSO was jointly sponsored by five organizations: the American Accounting Association, American Institute of CPA's, Financial Executives International, Institute of Internal Auditing, and the Institute of Management Accounting. In 1992, COSO issued a landmark report on internal control: *Internal Control—Integrated Framework*, which provides for establishing internal control systems and evaluating their effectiveness. In September 2004, COSO released *Enterprise Risk Management—Integrated Framework*, which provides guidance and standards

for implementing ERM. In 2017, COSO published an updated ERM framework, *Enterprise Risk Management: Integrating with Strategy and Performance*.

Crosscutting Risks: Risks that impact more than one line or staff office.

Cyber/Information Technology Risk: The broad risk associated with computers, business systems, e-commerce, on-line technology and increasingly other products and systems that are enabled by or rely on IT. Examples of technology risks include network/server failures, obsolescence, lack of IT resources/systems and skills, data breaches (to include personally identifiable information and protected health information), inadequate system security, viruses, denial of service, systems availability, and integration issues.

Elevate: To raise a risk to a higher level for managerial oversight.

Enterprise Risk Management (ERM): An effective agency-wide approach to addressing the full spectrum of an organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically aligned portfolio view of organizational challenges that provides improved insight about how to more effectively prioritize and manage risks to mission delivery.

Event: Occurrence or change of a particular set of circumstances.

Financial Risk: Risk that could result in a negative impact to the agency (waste or loss of funds/assets).

Government Performance and Results Act Modernization Act (GPRAMA): Requires that agencies revise strategic plans every 4 years and assess progress toward strategic objectives annually.

Hazard Risks: The risk that employee or organizational attitudes, conduct, or lack of awareness of hazards could impact the protection of lives and property and hinder efforts to prevent accidents and incidents. The risk that OIG will experience loss of critical functions caused by natural disasters, terrorist attacks, pandemics, or other hazards.

Human Capital Risk: Threats and opportunities associated with staff and management turnover; the employment/work culture; recruitment, retention, and staffing processes and practices; succession planning and talent management; and employee development, training, and capacity building.

Identify: Process of finding, recognizing, and describing risks.

Impact: Outcome of an event affecting objectives.

Inherent Risk: The exposure arising from a specific risk before any action has been taken to manage it beyond normal operations.

Internal Control: A management process that provides reasonable assurance that an organization will achieve its business/operations, financial reporting, and compliance objectives.

Key Performance Indicator: Key Performance Indicators (KPIs) are financial and nonfinancial metrics used to monitor changes in business performance in relation to specific strategic objectives.

Key Risk Indicator: Key Risk Indicators (KRIs) relate to a specific risk and demonstrate a change in the likelihood or impact of the risk event occurring.

Likelihood: The chance or probability of something happening.

Management Risks: The risks associated with ineffective, destructive, or underperforming management practices that hurt the organization's ability to meet its mission, goals, and objectives. This term refers to the risk of the situation in which the organization would have been better off without the choices made by management.

Mitigate: Strategy for managing risk that seeks to lower or reduce the significance and/or likelihood of a given risk.

Monitor: Process of reviewing changes to the risk baseline (risk profile) over time.

Operational Risk: The risk of direct or indirect loss arising from inadequate or failed internal processes, people and systems, or external events. It can cause financial loss, reputational loss, loss of competitive position, or regulatory sanctions.

Opportunity: A favorable or positive event. In context of risk management, it refers to the possibility that an event will occur and positively affect the achievement of objectives.

Organize: The process of defining the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for risk management policy.

Political Risk: Risk that may arise due to actions taken by Congress, the Executive Branch, or other key policy makers that could potentially impact business operations, the achievement of the agency's strategic and tactical objectives, or existing statutory and regulatory authorities. Examples include debt-ceiling impasses, government closures, etc.

Portfolio View: A composite view of risk that allows management to consider interdependencies and relationships across the organization.

Program Performance Risk: Threats and opportunities associated with an organization's process and practice of developing and managing major programs and projects in support of its overall mandate, as well as risks associated with specific programs or projects that may require ongoing management.

Reduction: Risk response where action is taken to reduce the likelihood or impact of the risk.

Report: The process of communicating risk information about the overall risk environment and individual risks to stakeholders, which is used to gauge the effectiveness of ERM.

Reporting Risk: The risk associated with the accuracy and timeliness of information needed within the organization to support decision-making and performance evaluation and outside the organization to meet standards, regulations, and stakeholder expectations.

Reputational Risk: Risk that a failure to manage risk, external events, and external media or to fail to fulfill the agency's role (whether such failure is accurate or perceived) could diminish the stature, credibility, or effectiveness of the agency. Reputational risk can arise either from actions taken by the agency or by third party partners including service providers and agents. Reputational Risk can also arise from negative events in one of the other risk categories such as Compliance Risk.

Residual Risk: The exposure remaining from an inherent risk after action has been taken to manage it, using the same assessment standards as the inherent assessment.

Resource Management Risks: Risk associated with the characteristics of how an organization operates. Risks may arise depending on the level of organizational effectiveness, including how people, processes, systems, finances, contracts, policies and procedures are leveraged to produce key deliverables or services.

Risk: The possibility that an event will occur and adversely affect the achievement of objectives. An effect is a deviation from the desired outcome, which may present positive or negative results.

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 in strategy setting and selecting objectives.

Risk Assessment: The identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed. Risk assessment involves evaluating the significance and likelihood of a risk, as well as any controls or other measures that mitigate or eliminate that risk.

Risk Assessment Score: A weighting of a potential outcome (positive/negative) multiplied by the probability of its occurrence and used to prioritize choices.

Risk Baseline: Initial risk inventory developed.

Risk Culture: The extent to which ERM is integrated into decision-making, including strategic planning, performance management, strategic decisions, tactical decisions, and transactions.

Risk Management Committee: A committee established with executive authority to take action to manage the risks that face the organization.

Risk Management Framework: A set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization.

Risk Owner: The person or entity with the accountability and authority to identify and respond to risks within a functional area.

Risk Profiles: Detailed documentation of risk statements and treatment strategies for the highest priority risks to an organization.

Risk Response: Management's strategy for managing (or responding to) a given risk. Risk response strategies include avoidance, sharing, reduction, transfer, and acceptance.

Risk Severity: Magnitude of a risk (High, Moderate, and Low) determined by considering the consequences and likelihood.

Risk Tolerance: The acceptable level of variation in performance relative to the achievement of objectives.

Risk Universe: A record of information describing all identified risks.

Severity: A measurement of considerations such as the likelihood and impact of events or the time it takes to recover from events.

Sharing: Risk response where action is taken to share risks across the organization or with external parties, such as insuring against losses.

Stakeholders: Threats and opportunities associated with an organization's partners and stakeholder demographics, characteristics, activities, and interests.

Strategic Risk: Risk that would prevent an area from accomplishing its objectives (meeting the mission).
Transfer: Risk response where action is taken to transfer risks across the organization or with external parties, such as insuring against losses or contracting activities.

Treat: Process of determining the appropriate response(s) to a risk (accept, mitigate, watch, research, elevate) and developing a corrective action plan and executing that plan. This is also known as risk treatment.

Uncertainty: The inability to know in advance the exact likelihood or impact of future events.

EXHIBIT G: REFERENCES

Committee of Sponsoring Organizations of the Treadway Commission *(2017). Enterprise Risk Management: Integrating with Strategy and Performance*. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2016). *Enterprise Risk Management: Aligning Risk with Strategy and Performance.* http://www.coso.org/

Council of the Inspectors General on Integrity and Efficiency (2012). *Quality Standards for Federal Offices of Inspector General*. https://www.ignet.gov/sites/default/files/files/Silver%20Book%20Revision%20-%208-20-12r.pdf

Department of Commerce (2013). *Enterprise Risk Management Guidebook*. Unpublished draft. GPRA Modernization Act of 2010, H.R. 2142, 111 Cong., (2010) https://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf

Gartner (2019). *Risk Identification and Assessment Essentials.* https://www.gartner.com/en/audit-risk/role/risk-leaders

HM Treasury (2004). *The Orange Book: Management of Risk, Principles and Concepts.* https://www.gov.uk/government/publications/orange-book

IBM Center for the Business of Government (2015). *Improving Government Decision Making Through Enterprise Risk Management.* http://www.businessofgovernment.org/report/improving-government-decision-making-through-enterprise-risk-management

LogicManager, Inc. (2016). *EBook: 5 Characteristics of the Best ERM Programs.* http://www.logicmanager.com/best-practice-erm-programs-ebook/

Office of the Inspector General, Pension Benefit Guaranty Corporation (2016). *OIG Enterprise Risk Management Program*. Unpublished memorandum.

Office of the Inspector General, U.S. Department of Labor (2019). *Fiscal Year 2018 Annual Performance Report & 2020 Annual Performance Plan.* https://www.oig.dol.gov/public/reports/FY_2018_Annual_Performance_Report.pdf

Office of the Inspector General, U.S. Department of Labor (2018). *Framework for Enterprise Risk Management.* https://www.oig.dol.gov/public/OIG%20DOL%20ERM%20Framework.pdf

Office of the Inspector General, U.S. Department of Labor (2018). *Strategic Plan Fiscal Years 2018-2022*. https://www.oig.dol.gov/public/reports/OIG%20Strategic%20Plan%202018-2022.pdf

Office of Management and Budget (2018). OMB Circular No. A-11, part 6, *Strategic Plans, Annual Performance Plans, Performance Reviews, and Annual Program Performance Reports.* https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

Office of Management and Budget (2016). OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control.* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf

Office of Management and Budget (2011). *Emergency Acquisitions Guide.* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/procurement_guides/emergency_acquisitions_guide.pdf

Protivity Inc. (2006). *Guide to Enterprise Risk Management: Frequently Asked Questions*. https://www.protiviti.com/US-en/insights/guide-erm-faq-j

Risk and Insurance Management Society, Inc. (RIMS) (2006). *RIMS Risk Maturity Model for Enterprise Risk Management.* https://www.logicmanager.com/pdf/rims_rmm_executive_summary.pdf

Sobel, Paul J. CPA, CIA (2015). *Auditor's Risk Management Guide, Integrating Auditing and ERM*.

Transportation and Security Administration (2014). *ERM Policy Manual*. https://www.aferm.org/wp-content/uploads/2015/10/TSA-ERM-Policy-Manual-August-2014.pdf

U.S. Chief Financial Officers Council & Performance Improvement Council (2016). *Playbook: Enterprise Risk Management for the U.S. Federal Government.* https://cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf

U.S. Government Accountability Office (2014). *Standards for Internal Control in the Federal Government (GAO-14-704G)* (Green Book). http://www.gao.gov/products/GAO-14-704G

U.S. Government and Accountability Office (2015). *A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP).* http://gao.gov/products/GAO-15-593SP

U.S. Government and Accountability Office (2015). *Managing for Results: Practices for Effective Strategic Reviews (GAO-15-602).* http://gao.gov/assets/680/671730.pdf

U.S. Government and Accountability Office (2016). *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risks (GAO-17-63).* https://www.gao.gov/assets/690/681342.pdf

U.S. Government Accountability Office (2018). *Government Auditing Standards, 2018 Revision (*Yellow Book*).* https://www.gao.gov/products/GAO-18-568G

Wright, Rick A. Jr., CIA (2018). *The Internal Auditor's Guide to Risk Assessment, Second Edition.*

EXHIBIT H: LIST OF PARTICIPATING OFFICES OF INSPECTOR GENERAL

OIGs for the following Federal agencies participated in the CIGIE ERM Working Group, and this practitioner's guide is the result of their collaboration.

1. Department of Agriculture
2. Department of Defense
3. Department of Education
4. Department of Health and Human Services
5. Department of Homeland Security
6. Department of Housing and Urban Development
7. Department of Labor
8. Department of State
9. Pension Benefit Guaranty Corporation
10. United States Agency for International Development