Office of Inspector General
U.S. Department of Labor

Framework for Enterprise Risk Management

Version 1.0

October 14, 2016

Inspector General

Deputy Inspector General

Chief Performance and Risk Management Officer

Table of Contents

Introduction

In order to deliver value to the nation, stakeholders, and our employees, we at the Office of the Inspector General (OIG), Department of Labor (DOL) must recognize, plan for and manage risks across our entire organization. Risk is defined as the effect of uncertainty on objectives, and can relate to strategic threats, operations, compliance with laws, and reporting obligations. If risks are not addressed at both the component and enterprise level, with attention to their interdependence and complexity, they can over time have significant and growing negative impacts on mission accomplishment. While we may be currently managing risks at various levels within the OIG, experience has shown the need to apply risk management at the enterprise level where risks and opportunities discussions are embedded in strategic planning, resource allocation, processes, and decision making. An enhanced level of enterprise risk management (ERM) maturity is essential for us to become a resilient organization that successfully addresses challenges due to an ever-changing federal landscape, as well as fully seize opportunities when presented.

This document provides an overview of our enterprise-wide approach to risk management (the "OIG Framework for Enterprise Risk Management" or "ERM Framework") and describes how we will implement this approach at the OIG. This framework version 1.0 aligns with the vision established by the Inspector General (IG) and Deputy Inspector General (DIG) and takes into account priorities outlined in external guidance such as the Office of Management and Budget (OMB)'s Circular A-123. This framework will continue to evolve as the Chief Performance and Risk Management Officer (CPRMO) collaborates with OIG leadership, staff and stakeholders from across offices and regions to mature the ERM function.

This version of the ERM Framework primarily provides a best-practice approach to identify and manage potential events that may impact the enterprise, as well as a basic governance and management structure to oversee and implement risk management activities. Some critical success factors for OIG's ERM Program include:

- Executive management engagement to:
    - Set the "tone at the top" and champion an OIG-wide risk culture
    - Establish priorities
    - Identify and respond to high-priority risks, including aligning resources to address risks
    - Mature OIG's ERM Program over time
    - Promote adoption of ERM through employee awareness and training
    - Integrate ERM with organizational performance management and strategic planning activities
- Stakeholder engagement at all levels
- Consistent communication of risk information
- Demonstrate value through "small wins"

It is expected that the applicability of ERM in the federal sector will evolve over time as lessons learned and best practices continue to be shared among federal ERM practitioners. It is critical that we implement a tailored ERM framework for the OIG that emphasizes trust, collaboration, continuous improvement, learning and growth among all members of our staff and our stakeholders.

OIG's Mission, Vision and Strategic Goals & Objectives

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.

Our approach to strategy and performance management is informed by requirements set forth by the Government Performance and Results Act Modernization Act of 2010, and OMB Circular A-11 Part 6. ERM will allow us to systematically consider risk in strategic planning, performance planning and reporting processes to ensure that our management of risk is appropriately aligned with our mission, goal, objectives and priorities.

OIG's Mission

We serve the American workforce, the Department of Labor, and the 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.

OIG's Vision

- Enhance through our oversight the ability of the Department of Labor to address emerging workforce challenges; and
- Foster a thriving work environment that values employees as our greatest asset.

OIG's Strategic Goals & Objectives

Goal 1: **Deliver timely, relevant, and high-impact results.**

- **Strategic Objective 1.1**: Strengthen DOL's key programs and operations through our work and other deliverables.
- **Strategic Objective 1.2**: Improve our work processes to drive the timely completion of relevant and impactful audits and investigations.
- **Strategic Objective 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.
- **Strategic Objective 1.4**: Timely articulate to our external stakeholders the relevance and impact of our work in each product.
- **Strategic Objective 1.5**: Proactively engage our key stakeholders to seek their input for identifying potential audits and investigations.

Goal 2: Foster an internal OIG culture that drives high performance and engagement.

- **Strategic Objective 2.1:** Promote transparent and timely communications that foster civility, respect and inclusiveness at all levels.

- **Strategic Objective 2.2:** Establish and implement transparent and effective policies and processes for promoting and rewarding staff, including clearly defined career ladders.
- **Strategic Objective 2.3:** Develop and implement strategic recruitment, succession, and retention plans.
- **Strategic Objective 2.4:** Develop and implement a formal mentoring program.
- **Strategic Objective 2.5**: Provide each employee with an opportunity to develop an employee development plan and encourage all employees to participate.
- **Strategic Objective 2.6:** Develop an objective exit interview process.
- **Strategic Objective 2.7**: Increase use of mechanisms for obtaining employee feedback, such as 360 degree evaluations and one-on-one sessions.
- **Strategic Objective 2.8**: Ensure training funds are used to maximize employee development.

Goal 3: Promote responsible stewardship of OIG financial and non-financial resources.

- **Strategic Objective 3.1**: Develop a sound budget based on operational needs and priorities.
- **Strategic Objective 3.2**: Manage workload to adapt quickly to changing and emerging resource requirements.
- **Strategic Objective 3.3**: Engage in outreach to the Department, the Congress, and OMB to demonstrate the value of our work.
- **Strategic Objective 3.4:** Leverage OIG technology to enhance audit, investigative, and administrative processes and deliverables.
- **Strategic Objective 3.5**: Ensure funds are monitored and used in a cost-efficient manner.

ERM will assist OIG leadership in defining the amount of risk we are willing to accept in pursuit of our mission, vision, values and strategic goals and objectives. Lack of clarity on our organizational risk appetite poses several risks. We may take risks well beyond our comfort level, not optimize resource allocation, or may forego strategic opportunities due to an implicit and culturally informed risk aversion. Integrating ERM into our organization will ultimately help enhance organizational performance by more closely linking strategy and objectives to both risk and opportunity.

Source: Committee of Sponsoring Organizations of the Treadway Commission, ERM Framework: Aligning Risk with Strategy and Performance

Value of Enterprise Risk Management

ERM refers to the culture, capabilities, and practices that organizations rely on to manage risk in creating, preserving, and realizing public value. As described in our mission and vision statements and strategic plan, the OIG creates public value when resources available to us are optimally deployed. Among the most important internal resources OIG marshals to realize public value are (1) people, (2) OIG core values, (3) capital assets, (4) effective policies and processes, and (5) our brand. OIG realizes public value when the public and stakeholders derive benefits that we enable or create. By implementing ERM capabilities coordinated with strategic planning, performance management, and internal controls processes we expect to improve mission delivery, reduce costs, and focus corrective actions towards key risks.

OIG Core Values

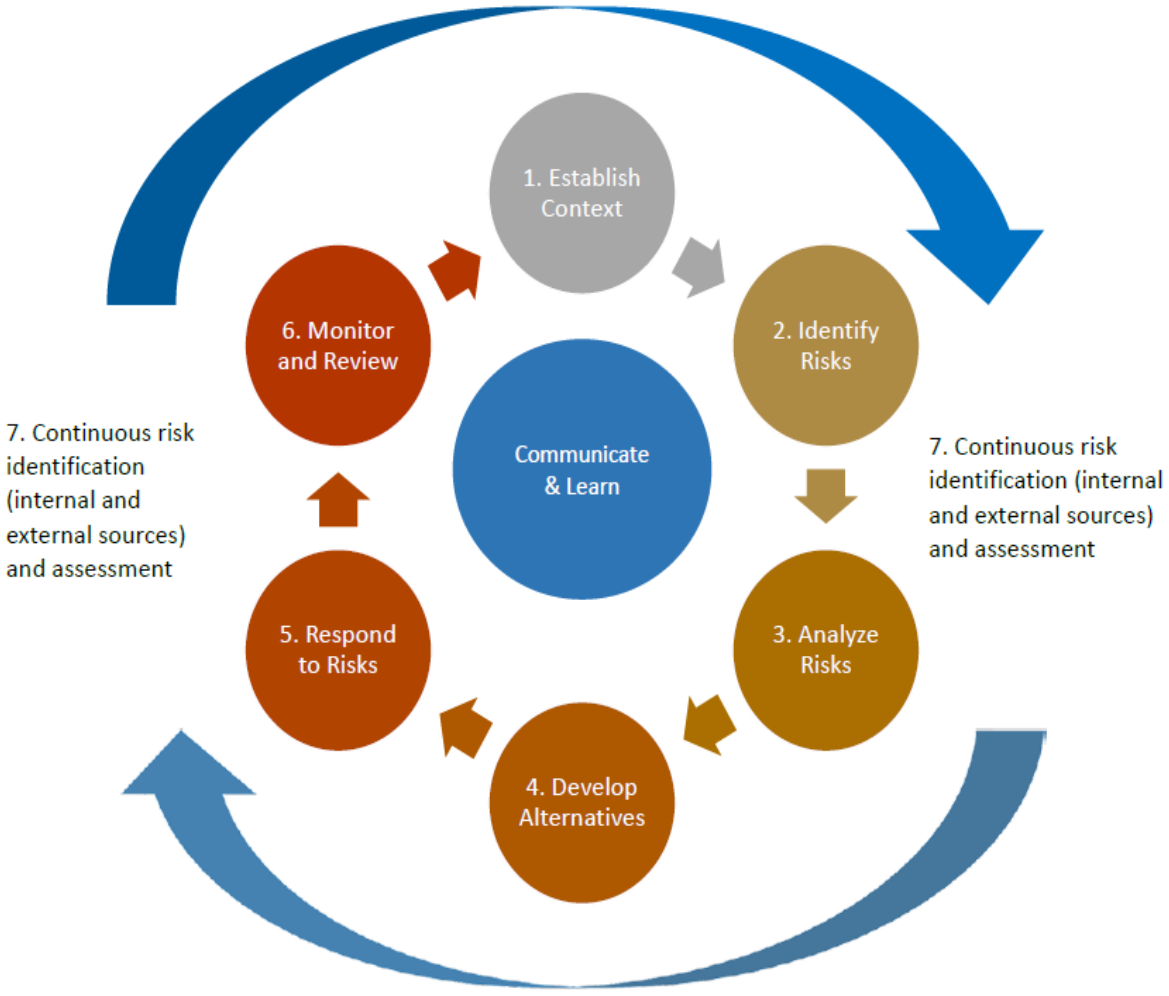
- **Excellence** - We deliver relevant, quality, timely, high-impact products and services, through a workforce committed to accountability and the highest professional standards.
- **Integrity** - We adhere to the highest ethical principles, and perform our work in an honest and trustworthy manner.
- **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.

The value of ERM stems from the IG and DIG's commitment to a culture that is people focused, process oriented and performance driven. Successful ERM implementation reinforces OIG's goal of creating a high performing, resilient organization by establishing an open, transparent culture that encourages people to communicate information about potential risks or other concerns with their superiors without fear of retaliation or blame. Our ERM program aligns with the OIG's Leadership Philosophy Statement (see Appendix A), and organizational structure (see Appendix D).

The value of ERM is also affirmed by our stakeholders. For example, the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Quality Standards for Federal Offices of Inspector General requires that "the IG should provide for an assessment of the risks the OIG faces from both external and internal sources." Also, the U.S. Government Accountability Office (GAO)'s Standards of Internal Control in the Federal Government, and OMB's Circular A-123 include detailed guidelines for the evaluation of systems of internal controls, and emphasize the need to manage risks and internal control in both financial and nonfinancial areas, and require federal agencies to implement ERM practices.

Components of the OIG's ERM Framework

Based on an assessment of 26 ERM program success factors developed by the Risk and Insurance Management Society, the OIG is currently at the "ad-hoc" or level 1 maturity stage. Our ERM framework is tailored to meet OIG's strategic objectives and seeks to progressively enhance our maturity level to the "leadership" or level 5 maturity stage. Our framework relies on key principles and best practices outlined in OMB Circular A-123, the Orange Book, Management of Risk – Principles and Concepts, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s Enterprise Risk Management Framework, GAO recommendations and other sources.



Source: Adapted from OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

As recommended by OMB Circular A-123, our ERM framework will leverage the following 7 steps:

Step 1: Establish the Context	Understanding and articulating the internal and external environments of the organization.
Step 2: Initial Risk Identification	Using a structured and systematic approach to recognizing where the potential for undesired outcomes or opportunities can arise.
Step 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.
Step 4: Develop Alternatives	Systematically identifying and assessing a range of risk response options guided by risk appetite.
Step 5: Respond to Risk	Making decisions about the best options(s) among a number of alternatives, and then preparing and executing the selected response strategy.
Step 6: Monitor and Review	Evaluating and monitoring performance to determine whether the implemented risk management options achieved the stated goals and objectives.
Step 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.

Source: OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

Step 1: Establishing the Context

The OIG was established at twelve federal agencies, including the DOL, by the Inspector General Act of 1978 in response to a series of government scandals that had occurred over the preceding decade. Congress believed that establishing independent Inspectors General (IGs) within these federal agencies would accomplish the following:

- Taxpayer dollars would be used more prudently and accurately accounted for;
- The government would be better equipped to prevent and detect fraud, waste, and abuse; and
- The public's confidence in their government would be enhanced.

The IG is nominated by the President and confirmed by the Senate, without regard to political affiliation and solely on the basis of integrity and demonstrated ability. The IG is non-political and, therefore, is subject to the Hatch Act. An IG may only be removed by the President, who must notify the Congress of the reasons for such removal.

The OIG conducts audits to review the effectiveness, efficiency, economy, and integrity of all DOL programs and operations, including those performed by its contractors and grantees. This work is conducted in order to determine whether: the programs and operations are in compliance with the

applicable laws and regulations; DOL resources are efficiently and economically being utilized; and DOL programs achieve their intended results.

The OIG also conducts criminal, civil and administrative investigations relating to violations of Federal laws, rules or regulations related to DOL programs and operations; as well as investigations of allegations of misconduct on the part of DOL employees. In addition, the OIG has an external program function to conduct criminal investigations to combat the influence of labor racketeering and organized crime in the nation's labor unions. We conduct labor racketeering investigations in three areas: employee benefit plans, labor-management relations, and internal union affairs.

The OIG creates public value to American workers, retirees and taxpayers by conducting audits and investigations that result in improvements in the effectiveness, efficiency and economy of Departmental programs and operations. The IG has authority to have direct and prompt access to the Secretary for any purpose relating to the performance of the OIG's mission and responsibilities. Also, the IG has the authority to select and appoint employees, directly contract for program services, maintain legal counsel who reports directly to the IG, and operate IT systems as a subdomain on the DOL enterprise domain. Our reporting mechanisms include:

- Meetings and briefings with departmental officials;
- Meetings with members of Congress and their staffs;
- Congressional testimony;
- The Semiannual Report to the Congress;
- Top Management Challenges Report; and
- A special transmittal to the Secretary on particularly serious or flagrant problems. The Secretary must then provide that report (often called a "7-day letter") to the Congress within seven days.

We develop our strategic work plan through consultations with stakeholders and others, including DOL management, Congressional committees, U.S. Attorneys, the Government Accountability Office (GAO), and other government entities. In addition, the Secretary and the Congress may request the OIG to perform an audit or investigation.

For audits, we prioritize the potential areas and, based on a risk assessment that considers program dollar size, vulnerability to abuse, potential impact on the public, and prior audit and investigative history, develop a comprehensive, coordinated strategy to address those high-priority areas. After consideration of the availability of staff resources and any planned initiatives of other government entities, we develop annual work plans of initiatives, and then share it with DOL management.

Program fraud investigations typically result from allegations or suspicions of wrongdoing involving DOL programs, operations or personnel. Also, they may be the result of broad initiatives arising out of prior OIG activities or as part of broad interagency initiatives, normally in consultation with the appropriate U.S. Attorneys.

Labor racketeering investigations give highest priority to traditional organized crime domination of labor unions and/or employee benefit plans. Priority is also given to cases where the perpetrators are not members of traditional organized crime, but can be considered (either by criminal background or the nature of the activity) to be professional criminals who have used a position of trust or control for criminal purposes.

Over the past three years, our organization experienced significant turnover in staff and leadership positions. In October 2013, a new IG was appointed, bringing a new leadership vision and strategic priorities. While the new vision is people centric, significant efforts are also underway to enhance organizational culture, processes, and program outcomes. In light of our mission, our leadership is committed to promoting conscientious management, being good stewards of our resources, as well as encouraging high standards of professionalism and integrity.

Step 2: Risk Identification

In order to manage risks, we need to know what risks we face and be prepared to evaluate them. The key objective of Step 2 is to identify a comprehensive list of risks and events that may potentially impact the achievement of OIG's mission and strategic objectives, as well as risks that can impact operational, reporting and compliance mandates. The initial risk identification process will be collaborative, leveraging interviews with subject matter experts (SME) and key personnel across the OIG in an effort to promote an organizational culture that encourages employees to identify and discuss risks openly. In addition, the risk identification process will include review of data such as, the Federal Employee Viewpoint Survey, workforce demographics and turnover information, and annual performance results. Efforts will lead to the creation of an initial risk profile which will identify, assess and prioritize our risk universe from an enterprise view. Once initial risks are identified by SME, we will re-examine them regularly to identify new risks or changes to existing ones.

The risk profile will serve as a baseline identifying risks by categories and subcategories, and capturing several of the framework process steps such as identification of risks, assessment of inherent risk, identification of risk response, assessment of residual risk, and identification of proposed actions. Risks will be identified and categorized based on the following four overarching categories (strategic, operations, reporting and compliance) and six risk subcategories (reputational, political, management, technological, resource management and hazard risks):

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; our ability to demonstrate and measure the effectiveness of our programs.

Strategic Risks Subcategories		
Reputational 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, DOL, employees,	**Political Risks** 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	**Management Risks** Risk that the OIG's management practices will impact its ability to meet mission goals and objectives. **Examples:** • Organizational structure • Decision-making

the public, Council of the Inspectors General on Integrity and Efficiency (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 DOL officials	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	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

Operations Risks:

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/damage to people or property, and/or impact to achieving OIG's mission, goals or objectives. Risks related to the effective and efficient use of OIG resources 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.

Operations Risks Subcategories		
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	**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	**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

inadequate • New or untried technologies that impact our current investments or activities • Network/server failures • Loss of data	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.	threats to any individual on site, due to an external threat or event • Utility failure • Health hazards • Cybersecurity threats • Lawsuits

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.

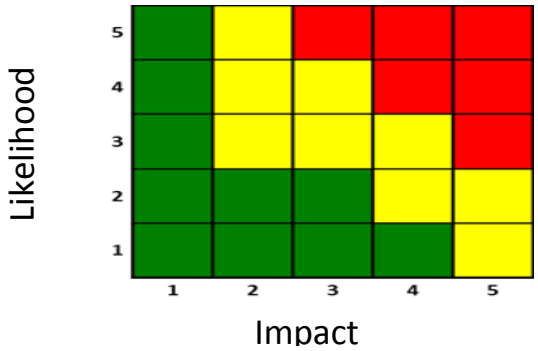
Examples:

- 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

These risk categories and subcategories are meant to aid OIG SME participating in the initial qualitative risk assessment interview process by considering a myriad of potential key risks triggers that may lie within each objective or category. Other sources of information useful in identifying risks include: (a) peer reviews, (b) Congressional hearings and meetings with Congressional staff highlighting interests and concerns, (c) issues and risks identified in the media, (d) appropriations language, (e) OIG and GAO reports, and (f) OIG's annual performance plans, and annual performance reports.

Step 3: Analyzing and Evaluating Risks

Our approach for analyzing and evaluating risks includes considering perspectives from a range of OIG staff, or stakeholders affected by the risks. The analysis will be done by evaluating the likelihood of the risk occurring and the impact if the risk is realized. We will consider inherent risk which is the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations, as well as residual risk (the risk after control has been applied which, assuming the control is effective, will be the actual exposure to the OIG) for all risks identified. We will leverage a standard 5x5 "heat map" to categorize and aggregate risks on a scale of 1 to 5. When conducting risk assessment scoring, most SME will use professional judgment to determine the probability and impact of risk events based on the likelihood and impact scales, and scoring criteria highlighted below:



Impact	Likelihood

(5) Very High: **D**egradation of an activity or role is **severe** impacting our ability to meet one or more strategic goal, objective, 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** and is 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**. .

Once inherent and residual risks have been assessed and scored for both impact and likelihood, we will multiply the values so that high risk priorities can be determined. The less acceptable it is for OIG to expose itself to a particular risk (see Appendix B "OIG's Risk Appetite Rating Scale"), the higher the priority which should be given to addressing the risk. The highest priority risks (the top 10 risks) will be given regular attention at the IG and DIG level, and will be fully integrated with strategic planning, organizational performance management processes, and resource allocation plans. The specific risk priorities will change over time as risks are identified and addressed, and organizational priorities evolve to meet mission needs.

Step 4: Developing Alternatives

Once the risks are scored and ranked, the IG and DIG will select the top 10 risks based on the risk appetite for the OIG. For these top 10 risks, we will systematically identify and assess a range of response options or strategies to avoid, accept, reduce or share risks. We will take into account the following: (a) weighing the cost of addressing the risk against the level of risk exposure, (b) the value of potential benefits, opportunities and loses, (c) the best way to allocate financial and non-financial resources, (d) non-financial considerations such as reputational capital at stake, and (e) determine whether or not control options can be effectively leveraged or modified to best respond to a given risk. Generally speaking, we will consider controls to manage risk rather than to eliminate it. When implemented, controls and resource allocations will be proportional to the risk.

Step 5: Responding to Risks

After conducting Steps 1 through 4, the IG and DIG will make determinations on how to best allocate scarce resources to address the top 10 risks. While the CPRMO will facilitate the process, managing risk is the responsibility of the Assistant Inspector General (AIG), and the Office head where the risk resides.

Our risk response strategies will consider the following options:

Risk Avoidance	**Discontinue** operations or activities in a particular area. **Prohibit** unacceptably high-risk activities and process exposures through appropriate policies and procedures. **Stop** specific activities by redefining objectives, refocusing strategic plans and policies, or redirecting resources. **Screen** alternative projects and budgeted investments to avoid off-strategy and unacceptably high-risk initiatives. **Eliminate** risks at the source by designing and implementing internal preventive processes.
Risk Acceptance	**Retain** risk at its present level, taking no further action
Risk Reduction	**Disperse** financial, physical, or information assets to reduce risk of unacceptable losses. **Control** risk through internal processes or actions that reduce the likelihood of undesirable events occurring to an acceptable level (as defined by management's risk tolerance). **Respond** to well-defined contingencies by documenting an effective plan and empowering appropriate personnel to make decisions; periodically test and, if necessary, execute the plan. **Diminish** the magnitude of the activity that drives the risk. **Isolate** differentiating characteristics of assets to reduce risk of loss through imitation, obsolescence, or other competitive pressures. **Test** strategies and implemented measures on a limited basis to evaluate results. **Improve** capabilities to manage desired exposure. **Relocate** operations in order to transfer risk from once component, in which it cannot be well managed, to another component that can. Diversify assets currently implemented for mission and business operations
Risk Sharing	**Outsource** process or activities through contractual arrangements. **Delegate** risk by entering into arrangements with independent, capable authorities.

Source: Adapted from the Transportation Security Administration's Enterprise Risk Management Policy Manual (2014)

The output of Step 5 will include risk response strategies and plans which will include analyzed costs and timelines for development and implementation. Also, this step will allow us to update the risk register with quantified residual risks.

Key Risk Indicators (KRI) may be developed in tandem with Key Performance Indicators (KPI) for inclusion in our OIG's Annual Performance Plans and Annual Performance Reports to demonstrate the interrelationship between risk and performance, as well as to predict whether a risk is materializing. Together, KPI and KRI support a proactive approach to performance management.

The CPRMO will monitor implementation of the risk management strategy and annual performance plans and will report progress to the IG and DIG no less than every 6 months. The IG and DIG may decide to adjust the approach for managing particular risks if implementation fails to bring the risk within desired limits.

Step 6: Monitoring and Review

We will monitor and review risks and communicate whether or not the risk profile is changing, and to gain assurance that risk management efforts are effective. The CPRMO will work with senior leadership to determine if identified risks still exists and ensure that risk management strategies are being carried out effectively in a timely manner. A variety of tools such as risk self-assessment questionnaires, templates, and IT systems (based on funding availability) may be used to conduct risk reviews. Reviews will occur at a frequency of no less than every 6 months.

Step 7: Continuous Risk Identification

The risk profile will be regularly updated based on continuous risk identification to capture changes (based on both internal and external factors) in existing risks, or to add risks which were not captured initially. Moreover, all aspects of the ERM program, including processes, tools and templates will be regularly reviewed and evaluated to determine if our strategies, objectives and organizational performance is optimized; whether our ERM practices are achieving the stated goals and objectives; and whether or not we are advancing our ERM maturity level. Staff and stakeholder feedback will be leveraged to pinpoint areas of improvement.

Governance and Oversight Structure

The IG and DIG with the support of the CPRMO, are responsible for managing the ERM program, and encouraging a risk-aware culture that promotes individual accountability at all levels of the organization. It is the responsibility of the Assistant Inspectors General (AIG) and other senior leaders to manage risks in their respective program areas, to include both mission critical and mission support functions. This includes identifying, analyzing and evaluating risks and opportunities, and presenting risk response options to the IG and DIG. All OIG employees are encouraged to be open, candid, and fact-based in discussing risk issues, making all relevant facts and information available so the IG and DIG can consider all options and make informed decisions. All OIG employees have a responsibility to speak candidly and escalate risk-related concerns to management. If an OIG employee prefers confidentiality or anonymity, the employee may report the risk concerns to the Employee Advisory Council (EAC).

The OIG's Risk Management Council (RMC) will serve as the governing body for ERM and will convene no less than every six months (see Appendix C "OIG Risk Management Council Charter"). The RMC membership will include:

- IG (Chair)
- DIG (Co-Chair)
- CPRMO (Convener)
- Counsel, Office of Legal Services
- AIG, Deputy AIG (DAIG), Office of Audits
- AIG, DAIG, Office of Labor Racketeering and Fraud Investigations
- AIG, DAIG, Office of Management and Policy
- Chief, Office of Special Investigations
- Director, Office of Congressional and Public Affairs
- Ombudsman (non-voting member)
- EAC Chair (non-voting member, by invitation only)

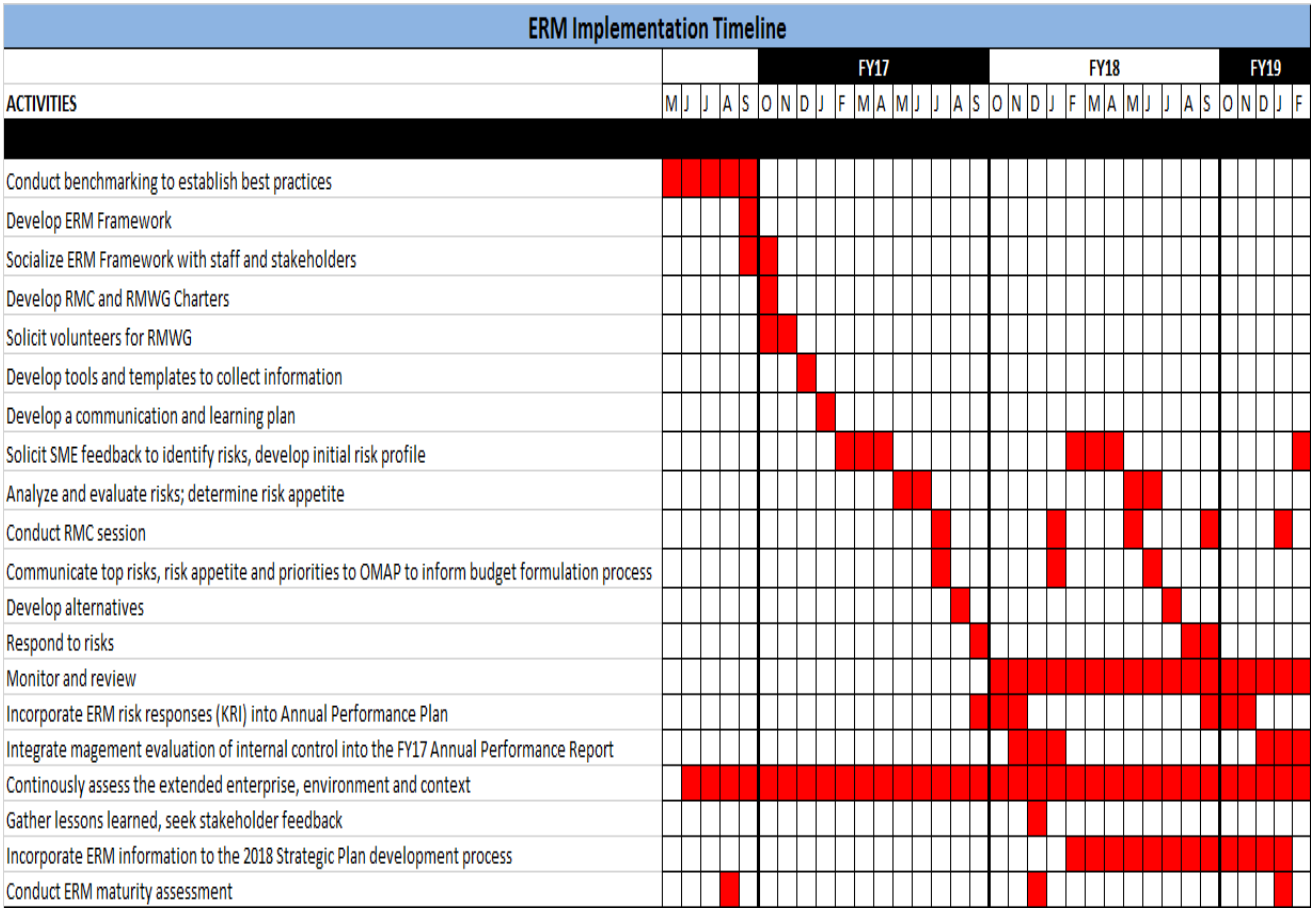
Responsibilities of the RMC include:

- Enable risk-informed decision-making
- Support the IG and DIG in establishing risk appetite for the OIG
- Identify high-priority risks and decide how to respond to them in concert with risk owners
- Support implementation of effective controls
- Identify emerging risks, concentrations of risk, and other situations that could be properly assessed
- Assess organizational performance
- Elevate critical issues in a timely fashion

In addition to the RMC, the CPRMO will create and oversee a Risk Management Working Group (RMWG) that will include diverse representatives from across the organization, including regions. The RMWG will build ERM capacity across the OIG, encourage communication and learning, disseminate best practices, and support a risk-aware culture among all staff. The RMWG representation will consist of volunteer staff with endorsements provided by each AIG or Office Director/Chief. The RMWG volunteer staff will be responsible for advancing the maturity of ERM within the OIG, including but not limited to: creating tools, templates, and training modules; issuing guidance as well as performing SME interviews; conducting risk analysis; soliciting stakeholder feedback; and support administrative duties, as needed.

ERM Implementation Timeline

Our ERM implementation timeline seeks to follow the spirit, requirements and timelines set forth in OMB Circular A-123 and other mandates. We plan to incorporate ERM findings into our FY19 budget formulation and performance management processes; FY18 strategic plan development efforts; as well as integrate management evaluation of internal controls in our FY17 Annual Performance Report.



Maturity Model

Based on an assessment of OIG ERM maturity level conducted in early August 2016, we have determined that our efforts are consistent with the "ad-hoc" maturity level characteristics. Our goal is to reach a level of "leadership" by the end of FY19. Progress will be assessed by soliciting yearly stakeholder feedback as part of OIG's RMC assessment process.

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 where 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 on-going 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, measurement 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.

Source: RIMS http://www.logicmanager.com/risk-maturity-model-rmm/

Conclusion

Changes in society, operations and technology have contributed to a versatile risk environment. The nature of risk is ever-evolving in government, and its dynamics originate from a variety of sources.

The adoption of ERM has grown in both private and public sector over the years as organizations are looking to build resiliency and adapt to change most effectively. The ERM approach is an important step in government's continual evolution and growth as it will enhance our ability to create public value while identifying opportunities and threats to the achievement of our mission and objectives.

OIG is committed to mature our ERM program. We will move our ERM initiative forward by linking our strategy, risk and organizational performance management process to ultimately grow the OIG into a high performing organization.

Appendix A: OIG Leadership Philosophy

OIG Leadership Philosophy

OIG leaders demonstrate daily the core value that employees are our greatest asset. We do this by providing our people with the leadership excellence that they deserve and modeling positive interpersonal qualities that we seek to instill throughout the organization.

We value the contributions of everyone and foster a culture of inclusiveness where each member is equally important. We encourage collaboration and self-expression from all so that we can achieve results more robust than would come from individual efforts alone.

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.

To empower and engage our people, we lead with humility, seek feedback, share information across the organization, delegate challenging work, and provide authority and autonomy for our people to succeed. We coach, not command and treat all with dignity, respect, and civility.

The success of our people is our primary objective. We set clear goals with our sights on results, focus on what is possible, and our words inspire everyone to do their best. We celebrate success and learn from failure. As leaders, we seek to develop staff and create future leaders.

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.

We pledge to accept and follow this philosophy as a description of how we operate and act, and to hold each other accountable for modeling this through our words, actions, and behavior.

Appendix B: OIG Risk Appetite Rating Scale

Risk appetite is the amount of risk the OIG is willing to accept in pursuit of public value. This includes avoiding risks that could have unacceptable negative impacts, while pursuing calculated risks that could have beneficial outcomes or opportunities.

By understanding our risk appetite, we will better align OIG resources in pursuit of our strategic goals and objectives. It will help define our organizational risk culture by capturing the norms and expectations that inform daily decisions by management and employees on how to best achieve our mission. As we implement ERM, we will leverage the following Risk Appetite Rating Scale to guide OIG leadership in determining the appropriate risk appetite for the organization, and well as support future strategic goal setting, and performance management activities.

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 other 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 include 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

Source: Adapted from GAO 17-63 "Selected Agencies' Experiences Illustrate Good Practices in Managing Risks"

Appendix C: OIG Risk Management Council Charter

PURPOSE.

The Risk Management Council ("RMC") serves as the Department of Labor, Office of Inspector General ("OIG") senior decision-making body related to risk management and organizational performance. The purpose of the RMC is: 1) to monitor the achievement of OIG's strategic goals and objectives; 2) to monitor activities and exposures for various risks across the OIG, including strategic, operations, reporting and compliance risks; 3) to monitor risk response strategies and resource allocation; and 4) to review risk governance structure, including risk management practices and related issues.

APPLICABILITY/SCOPE.

The scope and authority of the ERMC encompasses all risk management and organizational performance management activities conducted by the OIG.

MEMBERSHIP.

The RMC Chair retains the discretion to expand the membership or attendance at any RMC meeting for any particular matter. This could include other individuals the RMC Chair, or Co-Chair deems necessary to include in the RMC deliberations.

RMC Members: The following officials serve as RMC members and attend all RMC meetings:

- Inspector General (Chair)
- Deputy Inspector General (Co-Chair)
- Chief Performance and Risk Management Officer (Convener)
- Assistant Inspector General for Audits
- Assistant Inspector General for Investigations
- Assistant Inspector General for Management and Policy
- Counsel to the Inspector General
- Deputy Assistant Inspector General for Audits
- Deputy Assistant Inspector General for Investigations
- Deputy Assistant Inspector General for Management and Policy
- Director, Office of Congressional and Public Affairs
- Chief, Office of Special Investigations.
- Ombudsman (non-voting member)[1]
- Employee Advisory Committee (EAC) Chair (non-voting member, will attend by invitation only)[2]

[1] The Ombudsman is an independent, neutral, confidential and informal resource available to all OIG employees experiencing interpersonal or organizational challenges. To preserve this independence and neutrality, Ombudsman's membership in the RMC will exclude voting on key issues.

[2] The EAC provides OIG employees with an avenue to raise important issues directly to the Inspector General and Deputy Inspector General. RMC membership for the EAC will be by invitation only, based on topics of discussion, and as requested by the Chair and Co-Chair. Moreover, the EAC membership will exclude voting on key issues.

RMC MEMBERS DUTIES AND RESPONSIBILITIES.

Assistant Inspector Generals (AIG) and managers are responsible for assessment, monitoring and management of risks within their respective program areas; as well as organizational performance. All AIG and managers shall demonstrate transparency and candor when discussing risk or performance issues, making all relevant facts and information available to the RMC. The RMC will rely on risk, performance reviews, information and reports provided by AIGs and management, and other sources of data to inform discussions and decisions.

The Council shall have the following duties and responsibilities:

- Support Chair decisions regarding risk appetite for the OIG
- Review progress made towards achieving OIG's strategic goals and objectives
- Review risk management activities used to measure, monitor and manage risks, and make recommendations on acceptable levels of risk exposure
- Review risk response options, as well as risk action plans and milestones
- Review existing internal controls and make recommendations for improvement
- Advise AIG and supervisors on the development and implementation of risk management activities
- Discuss OIG-wide risk management practices, and help develop best practices
- Address decisions of significant strategic direction and allocation of resources.
- Address any other issues at the discretion of the RMC Chair.

MEETINGS.

The RMC will strive to meet at least every 6 months. The Co-Chair or Convener will call meetings of the RMC. A majority of the Members for the RMC present at the meeting shall constitute a quorum. The agenda will be coordinated by the Convener, in consultation with the Chair and Co-Chair.

- Minutes. The Convener shall be responsible for facilitating the preparation and distribution of meeting minutes
- Agenda. The Convener shall provide Members the meeting agenda at least 48 hours in advance of the meeting.
- Attendance. Whenever appropriate, managers and their supervisors will be invited to attend meetings of the RMC at which their programs are being discussed, or those where their expertise would be helpful to RMC discussions.

STAFFING.

The Convener is responsible for facilitating support to the RMC at the direction of the Chair and Co-Chair, including facilitating administrative activities such as preparation of meetings minutes, as appropriate, in connection with the work of the RMC.

DURATION.

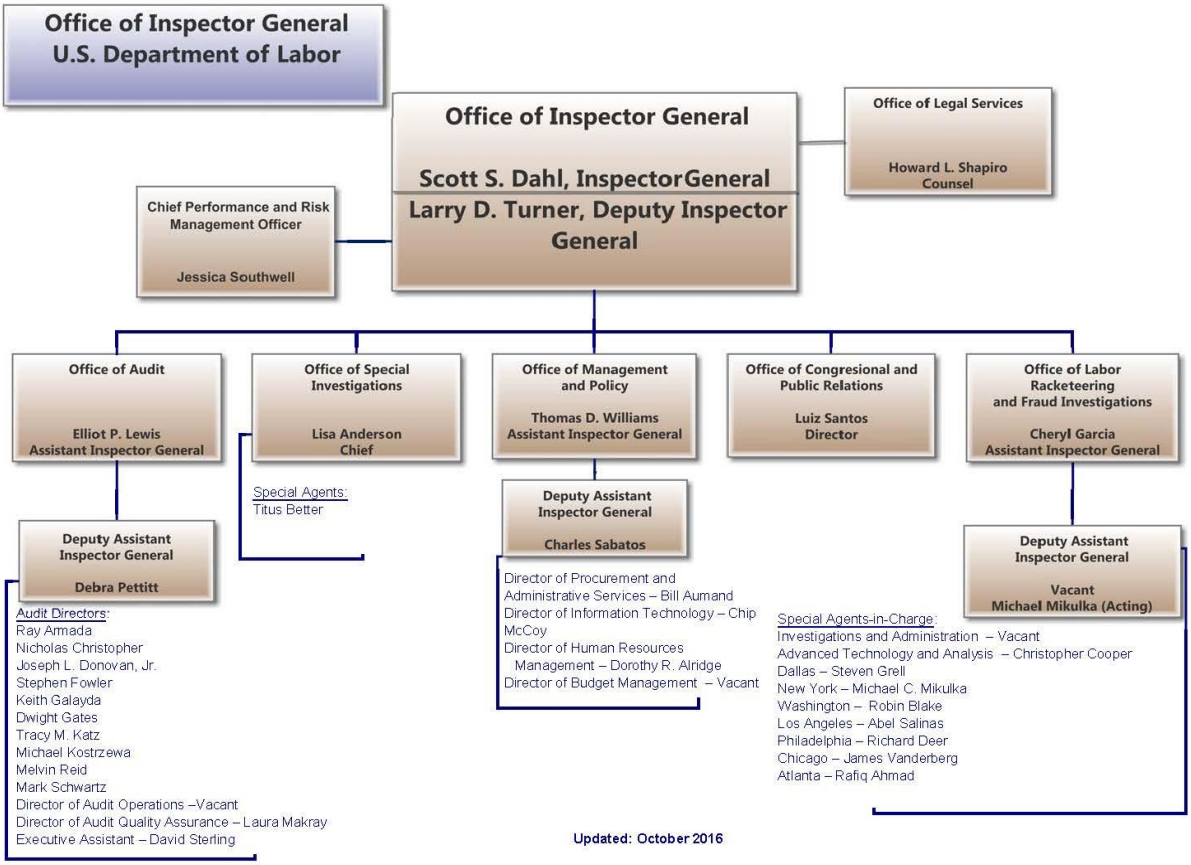
The RMC will remain in existence indefinitely.

ASSESSMENT.

An assessment of the RMC's progress in achieving objectives set forth in this Charter will be conducted by the Convener yearly. The assessment will be performed by conducting a yearly stakeholder feedback survey, including the following:

a. Level of effectiveness and outcome of decisions and recommendations made by the RMC
b. Level of inclusiveness and transparency demonstrated by Members and participants
c. Whether or not Members, AIGs and managers are promoting candid, fact-based discussion of risks and issues
d. Level of ERM maturity
e. Availability of data and key information to enable decision making
f. Recommendations for continuous RMC improvement.

Appendix D: OIG Organizational Chart



Glossary

A-123: Refers to OMB Circular No. A-123, which defines management's responsibility for internal control in Federal agencies. In Federal Student Aid, it often is used to refer to Appendix A of A-123, which includes specific requirements relating to internal control over financial reporting, and directs management to become more proactive in overseeing internal controls related to financial reporting.

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.

Avoidance: Risk response where 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 of 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.

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

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 the 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 four 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 (KRI's) relate to a specific risk and demonstrate a change in the likelihood or impact of the risk event occurring.

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: 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 which positions management to consider interdependencies and relationships across the organization

Likelihood: The chance or probability of something happening

Management Risks: The risks associated with ineffective, destructive or underperforming management practices, which hurts 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.

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: 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, as well as, 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 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 risks.

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 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 which 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).

Technology Risk: The broad risk associated with computers, e-commerce, and on-line technology. Examples of technology risks include: network/server failures, obsolescence, lack of IT resources/systems and skills, loss/theft of client/customer data, inadequate system security, viruses, denial of service, systems availability, and integration issues.

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), developing a corrective action plan and executing that plan; also known as risk treatment.

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

References

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

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. (2016). *Annual Performance Report Fiscal Year 2015. http://www.oig.dol.gov/public/reports/FY%202015%20Performance%20Report.pdf*

Office of Management and Budget. (2016). OMB Circular No. A-11 Part 6, *Strategic Plans, Annual Performance Plans, Performance Reviews, and Annual Program Performance Reports.* https://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc

Office of Management and Budget. (2016). OMB Circular No. 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

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

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).* 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).* Unpublished draft.

Bibliography

Bryson, John M., St*rategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement*. San Francisco: John Willey & Sons, 2004. Print.

DeLuca, Joel R. *Political Savvy: Systemic Approaches to Leadership Behind-the-Scenes*. Pennsylvania: EBG Publications, 1999. Print.

Hardy, Karen, *Enterprise Risk Management: A Guide for Government Professionals.* San Francisco: John Willey & Sons, 2015. Print.

Kettl, Donald F., *Escaping Jurassic Government: How to Recover America's Lost Commitment to Competence*. Washington, D.C.: Brookings Institution Press, 2016. Print.

National Aeronautics and and Space Administration: *Improvements to Current Processes for Risk Management at NASA: Roles and Responsibilities in Risk-Acceptance Decision-Making*. 2016. Washington, D.C. Unpublished draft.

National Aeronautics and Space Administration: *NASA Risk Management Handbook*. Washington, D.C. 2011. Print.

Partnership for Public Service & Grant Thornton, LLP: *Walking the Line: Inspectors General Balancing Independence and Impact.* Washington, D.C. 2016.

Rogers, Everett M., *Diffusion of Innovations*. New York: The Free Press, 1995. Print.

Segal, Sim, *Corporate Value of Enterprise Risk Management: The Next Step in Business Management.* New Jersey: John Wiley & Sons, 2011. Print.

Wholey, Joseph S., Newcomer, Kathryn E., *Improving Government Performance: Evaluation Strategies for Strengthening Public Agencies and Programs.* San Francisco: Josey-Bass, Inc. Publishers, 1989. Print.

Zaffron, Steve & Logan, Dave, *The Three Laws of Performance: Rewriting the Future of Your Organization and Your Life*. San Francisco: Josey-Bass, Inc. Publishers, 2009. Print.