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 five years, our organization experienced significant turnover in staff and leadership positions. A new IG was appointed in early 2022 and a new DIG selected shortly thereafter, 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. Our initial risk identification process was 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 included review of data such as, the Federal Employee Viewpoint Survey, workforce demographics and turnover information, and OIG annual performance plans and annual performance reports.[14] Efforts led to the creation of an initial risk profile from which OIG identified, assesses and prioritized our risk universe from an enterprise view. Since our initial risk identification process, OIG has regularly re-examined them—at least once every other year—to identify new risks or changes to existing ones.

OIG's risk profile serves as a baseline identifying risks by categories and subcategories, and captures 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. We identified and categorized risks based on the following four overarching categories and six risk sub-categories:

- Strategic
    - Reputational
    - Political
    - Management
- Operations
    - Technological

[14] Please see the OIG's FY 2021 Performance Report & FY 2023 Performance Plan at: https://www.oig.dol.gov/public/reports/FINAL__28-January-2022__FY%202021%20Annual%20Performance%20Report.pdf

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 aided 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 leveraged by SME in identifying risks included: (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, (f) OIG annual performance plans and annual performance reports,[15] and professional judgement.

STEP 3: ANALYZING AND EVALUATING RISKS

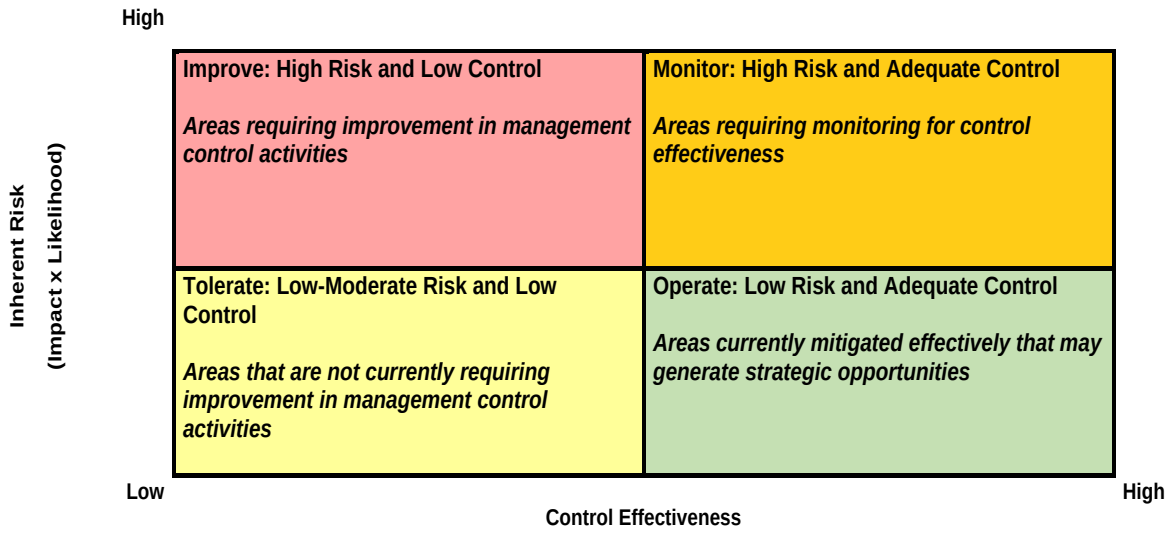
Our approach for analyzing and evaluating risks included considering perspectives from a range of OIG staff, or stakeholders affected by the risks. The analysis was done by evaluating the likelihood of the risk occurring and the impact if the risk is realized. We considered inherent risk (the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations), as well as residual risk (the risk assessed after applying internal controls and level of effectiveness, which represent the actual exposure to the OIG) for all risks identified.

When conducting risk assessment scoring, SMEs used professional judgment to determine the probability and impact of risk events based on the likelihood and impact scales, effectiveness of internal controls and scoring criteria as highlighted below:

Impact	Likelihood	Control Effectiveness
		(6) No controls in place: 0 percent controlled.
(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.**	**(5) Controls are ineffective, ad hoc:** 1 – 30 percent controlled.
(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.**	**(4) Controls are somewhat ineffective:** 31 – 55 percent controlled.
(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**.	**(3) Controls are effective:** 56 – 75 percent controlled.
(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.**	**(2) Controls are very effective:** 76 – 90 percent controlled.
(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**. .	**(1) Controls are extremely effective:** 91 – 100 percent controlled.

[15] Please see the OIG's FY 2021 Performance Report & FY 2023 Performance Plan at: https://www.oig.dol.gov/public/reports/FINAL__28-January-2022__FY%202021%20Annual%20Performance%20Report.pdf

Once inherent risks were assessed and scored for both impact, likelihood, and control effectiveness, we developed an inherent risk and control index (IRCI)—impact X likelihood X control effectiveness—and categorized risks based on 4 risk response options: operate, tolerate, monitor, and improve.



In addition, we evaluated all residual risks to identify risks that meet the definition of fraud as defined in GAO's Standards for Internal Control in the Federal Government ("Green Book").[16] We compiled and mitigated fraud risks derived from the ERM identification, analysis and evaluation steps as required by the Fraud Reduction and Data Analytics Act of 2015.[17] The less acceptable it is for OIG to expose itself to a particular risk, the higher the priority for addressing the risk. We give risks with the highest priority regular attention at the IG and DIG level, integrating such risks with strategic planning, performance management processes; and resource allocation plans. Risk priorities will change over time as risks are managed and organizational priorities evolve to meet mission needs. Please see Appendix E for additional details.

STEP 4: DEVELOPING ALTERNATIVES

Once we scored and ranked risks, the IG and DIG selected the top risks based on the risk appetite for the OIG, and leadership priorities. For these top risks, we systematically identified and assessed a range of response options or strategies to avoid, accept, reduce or share risks. In particular, we took into account the following: (a) cost of addressing the risk against the level of risk exposure; (b) value of potential benefits, opportunities and loses; (c) potential allocation financial and non-financial resources; (d) reputational capital at stake; and (e) whether or not control options can be effectively leveraged or modified to best respond to a given risk. To the maximum extend, we considered controls to manage risk rather than to eliminate it. When implemented, controls and resource allocations will be proportional to the risk.

[16] https://www.gao.gov/products/gao-14-704g
[17] https://congress.gov/114/plaws/publ186/PLAW-114publ186.pdf

STEP 5: RESPONDING TO RISKS

After conducting Steps one through four, the IG and DIG made determinations on how to best allocate scarce resources to address top risks. While the CPRMO and OPRM 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 considered 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 included risk response strategies and plans, which included analyzed costs and timelines for development and implementation. In addition, this step allowed us to update the risk register with quantified residual risks.

We incorporated Key Risk Indicators (KRI) or milestones associated with risk response plans with KPIs for inclusion in OIG's annual performance plans and annual performance reports.[18] This demonstrated the interrelationship between risk and performance, as well as help predict whether a risk is materializing. Together, KPI and KRI support a proactive approach to organizational performance management.

The CPRMO and OPRM monitor implementation of the risk management strategy and annual performance plans, and report progress to the IG and DIG 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 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 and OPRM 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.

The OIG uses IGRisk, which integrates OIG's enterprise risk data with organizational performance information in IGStat. IGRisk provides a variety of dashboards and analytical tools in a user-friendly format available to Executives on demand. We continue to use additional tools such as risk self-assessments and templates, as needed.

Reviews will occur at a frequency of no less than every six months.

STEP 7: CONTINUOUS RISK IDENTIFICATION

We review and update the risk profile regularly based on continuous risk identification. This allows us to capture changes (based on both internal and external factors) in existing risks, or to add risks not captured initially. Moreover, we regularly evaluate all aspects of the ERM program, including processes, tools and templates; whether our ERM practices are achieving the stated goals and objectives; and whether or not we are advancing our ERM maturity level. We also leverage staff and stakeholder feedback to pinpoint areas of improvement.

GOVERNANCE AND OVERSIGHT STRUCTURE

The IG and DIG with the support of the CPRMO and OPRM 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 AIGs 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

[18] Please see the OIG's FY 2021 Performance Report & FY 2023 Performance Plan at: https://www.oig.dol.gov/public/reports/FINAL__28-January-2022__FY%202021%20Annual%20Performance%20Report.pdf

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 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

The OIG Leadership Philosophy

Lead By Example * Trust and Value Others * Empower and Engage

We expect each OIG Manager to model our leadership values and behaviors, and recognize and support that you, our employees, are our most valued asset.

Our Leadership Philosophy guides our actions, our behaviors, and our thoughts throughout the OIG *at all levels* as we build an OIG culture that makes *everyone* feel like a member.

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—MODEL TOP C4

Model Top C4

Lead By Example * Trust and Value Others * Empower and Engage

We expect each OIG Manager to model our leadership values and behaviors, and recognize and support that you, our employees, are our most valued asset.

Our Leadership Philosophy guides our actions, our behaviors, and our thoughts throughout the OIG *at all levels* as we build an OIG culture that makes *everyone* feel like a member.

Model Leadership Philosophy through Words, Actions and Behavior

Operate with Staff's Best Interests in Mind

Develop Staff and Create Future Leaders

Employees Greatest Asset and Everyone Contributes

Leaders are approachable, empathetic, ethical, fair, transparent, and truthful; Leaders Exude Excellence; Lead with Humility, Seek Feedback, Share Information, Delegate Challenging Work, Provide Authority and Autonomy

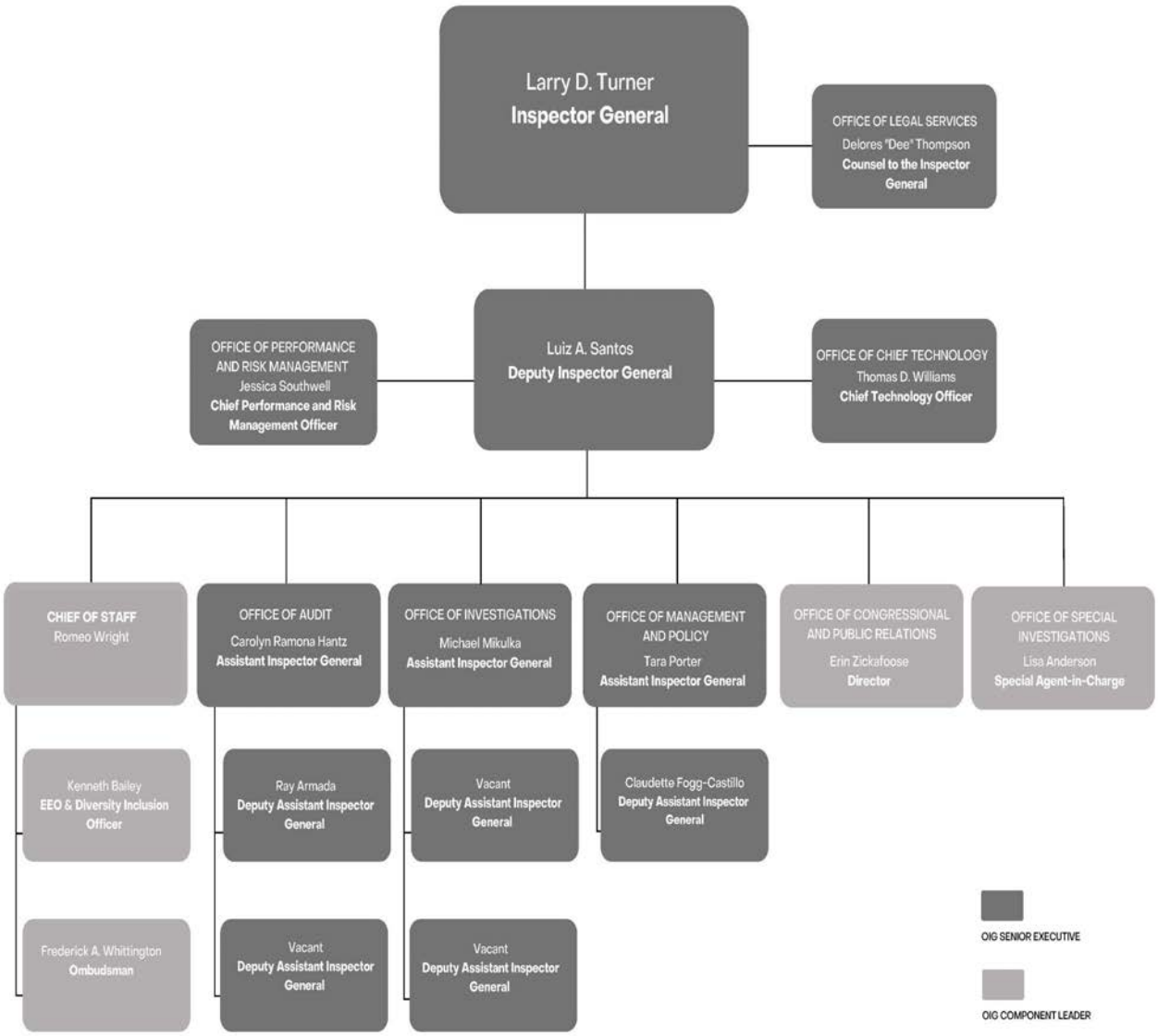
Teams Achieve Robust Results

Operate with Staff's Best Interests in Mind

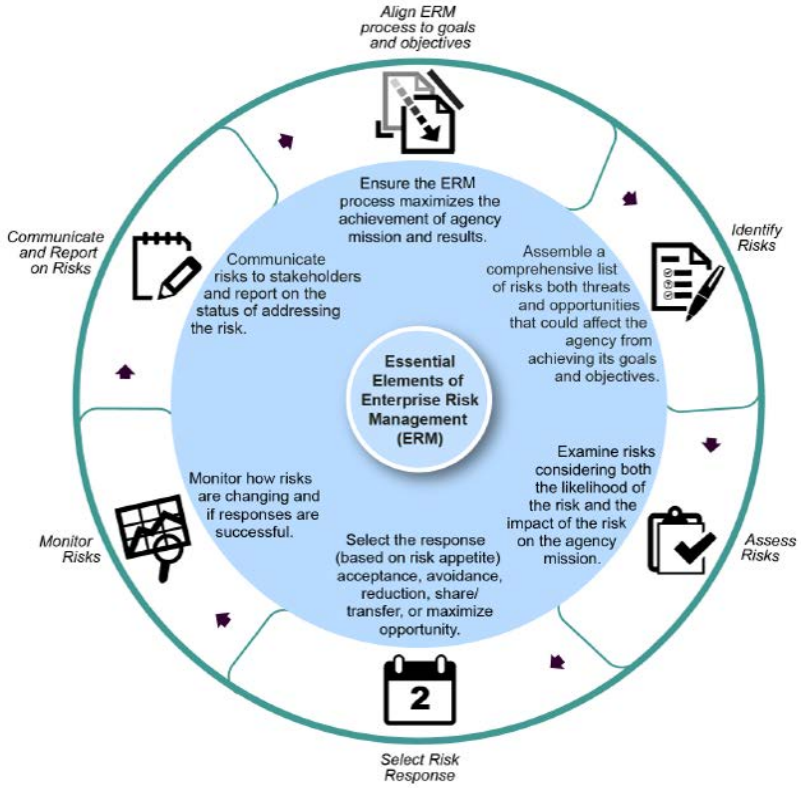
Positive Interpersonal Qualities

Clear Goals with a Focus on Results and the Positive
Coach While Treating Staff With Dignity, Respect and Civility
Collaboration and Self Expression Encouraged
Culture of Inclusiveness

APPENDIX C—OIG ORGANIZATIONAL STRUCTURE



APPENDIX D—GAO, KEY ELEMENTS OF ENTERPRISE RISK MANAGEMENT FRAMEWORKS



Source: GAO. | GAO-17-63

Table 1: Essential Elements and Associated Good Practices of Federal Government Enterprise Risk Management (ERM)

Element	Good Practice
Align ERM process to goals and objectives *Ensure the ERM process maximizes the achievement of agency mission and results.*	**Leaders Guide and Sustain ERM Strategy** Implementing ERM requires the full engagement and commitment of senior leaders, which supports the role of leadership in the agency goal setting process, and demonstrates to agency staff the importance of ERM.
Identify Risks *Assemble a comprehensive list of risks, both threats and opportunities, that could affect the agency from achieving its goals and objectives.*	**Develop a Risk-Informed Culture to Ensure All Employees Can Effectively Raise Risks** Developing an organizational culture to encourage employees to identify and discuss risks openly is critical to ERM success.
Assess Risks *Examine risks considering both the likelihood of the risk and the impact of the risk to help prioritize risk response.*	**Integrate ERM Capability to Support Strategic Planning and Organizational Performance Management** Integrating the prioritized risk assessment into strategic planning and organizational performance management processes helps improve budgeting, operational, or resource allocation planning.
Select Risk Response *Select risk treatment response (based on risk appetite) including acceptance, avoidance, reduction, sharing, or transfer.*	**Establish a Customized ERM Program Integrated into Existing Agency Processes** Customizing ERM helps agency leaders regularly consider risk and select the most appropriate risk response that fits the particular structure and culture of an agency.
Monitor Risks *Monitor how risks are changing and if responses are successful.*	**Continuously Manage Risks** Conducting the ERM review cycle on a regular basis and monitoring the selected risk response with performance indicators allows the agency to track results and impact on the mission, and whether the risk response is successful or requires additional actions.
Communicate and Report on Risks *Communicate risks with stakeholders and report on the status of addressing the risk.*	**Share Information with Internal and External Stakeholders to Identify and Communicate Risks** Sharing risk information and Incorporating feedback from internal and external stakeholders can help organizations identify and better manage risks, as well as increase transparency and accountability to Congress and taxpayers.

Source: GAO. | GAO-17-63

APPENDIX E—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 “Enterprise Risk Management: Selected Agencies’ Experiences Illustrate Good Practices in Managing Risks.”

APPENDIX F—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 RMC 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 – Labor Racketeering and Fraud
- Assistant Inspector General for Management and Policy
- Assistant Inspector General, Office of Congressional and Public Relations
- Counsel to the Inspector General
- Deputy Assistant Inspector General for Audits
- Deputy Assistant Inspector General for Investigations – Labor Racketeering and Fraud
- Deputy Assistant Inspector General for Management and Policy
- Chief, Office of Special Investigations
- Chief Technology Officer
- Ombudsman (non-voting member)[19]
- Employee Council (EC) Chair (non-voting member, will attend by invitation only)[20]

[19] 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.
[20] The EC provides OIG employees with an avenue to raise important issues directly to the Inspector General and Deputy Inspector General. RMC membership for the EC will be by invitation only, based on topics of discussion, and as requested by the Chair and Co-Chair. Moreover, the EC 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 Convener, in consultation with the Chair and Co-Chair, will coordinate the agenda.

- 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

The Convener will assess the RMC's progress in achieving objectives set forth in this Charter 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

GLOSSARY

A-11, Part 6: Refers to OMB Circular No. A-11, Part 6, which requires agencies are required to submit strategic plans, annual performance budgets, and annual program performance reports to the President, Congress, and OMB.

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.

IGRisk: OIG's automated ERM system. IGRisk is a unique system that integrates OIG's enterprise risk data with performance information from IGStat. The system also provides a variety of dashboards and analytical tools in a user-friendly format available to Executives on demand.

IGStat: OIG's automated organizational performance management system. IG Stat leverages OIG's organizational performance information to provide real-time updates to OIG leadership, conduct quarterly performance and leadership reviews, direct performance and risk assessments, and create reports such as the Annual Performance Report. The system also provides a variety of dashboards and analytical tools in a user-friendly format available to Executives on demand.

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. (2020). 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. (2022). *FY 2021 Performance Report & FY 2023 Performance Plan.* https://www.oig.dol.gov/public/reports/FINAL__28-January-2022__FY%202021%20Annual%20Performance%20Report.pdf

Office of Management and Budget. (2021)[21]. OMB Circular No. A-11 Part 6, *Federal Performance Framework for Improving Program and Service Delivery.* https://www.whitehouse.gov/wp-content/uploads/2018/06/part6_executive_summary.pdf

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/wp-content/uploads/legacy_drupal_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-enterprise-risk-management

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

[21] OMB rescinded Circular A-11, Part 6 in its entirety effective December 23, 2020. OMB reinstated Circular A-11, Part 6 in its entirety on March 24, 2021. For additional details, please see OMB Memorandum-21-22 found at: https://www.whitehouse.gov/wp-content/uploads/2021/03/M-21-22.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).* https://www.gao.gov/assets/690/681342.pdf

BIBLIOGRAPHY

Bryson, John M., S*trategic 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 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.

CONTACTS

Office of Performance and Risk Management

Jessica Southwell

Chief Performance and Risk Management Officer

southwell.jessica@oig.dol.gov

Heather T. Atkins

Senior Performance and Risk Analyst

atkins.heather@oig.dol.gov