## Contents

Overview ........................................................................................................................................................................ 3  
OIG’s Enterprise Risk Management Approach ................................................................................................................. 6  
  Phases in the Enterprise Risk Management Cycle ......................................................................................................... 7  
  Governance of OIG’s Enterprise Risk Management Program ......................................................................................... 16  
Enterprise Risk Management Program Maturity ............................................................................................................... 18  
Appendix A: OIG Vision, Mission, and Values .................................................................................................................. 19  
Appendix B: OIG Strategic Plan Goals and Objectives for FYs 2019-2022 ........................................................................ 20  
Appendix C: Enterprise Risk Management Maturity Model .............................................................................................. 21
OVERVIEW

This framework outlines the Office of Inspector General’s (OIG) approach for implementing its Enterprise Risk Management (ERM) program. This framework is informed by practices identified by the Council of the Inspectors General on Integrity and Efficiency for offices of inspectors general seeking to develop and implement their own ERM program.\(^1\) OIG intends to revise and reissue this framework as OIG’s ERM program evolves and matures.

Federal Agencies Required to Implement Enterprise Risk Management

In 2016, the Office of Management and Budget (OMB) issued its revised Circular No. A-123,\(^2\) which established ERM as a requirement for Federal agencies. As defined in the circular, ERM is an agency-wide approach to addressing the full spectrum of the organization’s external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. Consistent with OMB guidance, the Department of State (Department) established an ERM program and associated governance structure, which is outlined in 2 Foreign Affairs Manual 032. OIG is not included in the Department’s ERM governance structure for reasons of independence\(^3\) and, consistent with the practice of other offices of inspectors general, has chosen instead to establish its own ERM program. For the purposes of OIG’s ERM program, the enterprise is OIG. OIG’s Office of Enterprise Risk Management is charged with developing and managing OIG’s ERM program. The ERM office also leads OIG’s corporate processes related to strategic planning, performance management, and enterprise-wide policy.

OIG’s ERM program reflects OIG’s mission to conduct independent oversight of the Department, U.S. Agency for Global Media (USAGM), and U.S. International Boundary and Water Commission (USIBWC).\(^4\) OIG defines risk as the effect of uncertainty on an organization’s ability to meet its objectives. The definition is broad and includes, among other things, risks to achieving strategic goals, conducting internal operations, and maintaining compliance with laws, regulations, and policies. It also includes risks associated with failing to exploit opportunities to improve OIG’s effectiveness and efficiency. ERM requires coordinated activities to detect, monitor, and respond to the full constellation of risks, challenges, and threats OIG faces. It includes determining which risks are acceptable, which are not, and how resources should be allocated to prevent or mitigate those risks.

---

\(^1\) Council of the Inspectors General on Integrity and Efficiency, Enterprise Risk Management: Practitioner’s Guide for Offices of Inspectors General, October 2019.


\(^4\) See Appendix A for OIG’s Mission, Vision, Values statement.
Framework Establishes Approach for Implementation of Enterprise Risk Management at OIG

This framework establishes a structured approach to facilitate the implementation and operation of OIG’s ERM program. Specifically, this framework illustrates how enterprise risks have both short- and long-term effects on OIG’s oversight mission and internal operations. When implemented, this framework will enable OIG to identify and respond to risks that threaten OIG’s ability to execute its mission and achieve strategic goals. Moreover, this framework seeks to:

- Provide a common risk language so all OIG employees speak the same language when discussing and managing risks;
- Establish processes and a governance structure that promotes the early identification, assessment, and management of enterprise risks; and
- Embed risk management within OIG’s corporate processes to ensure that risks can be managed effectively.

As OIG’s ERM program accrues risk-related data and matures, OIG will refine its ERM processes. Accordingly, this framework will evolve to reflect the maturity of OIG’s ERM program as well as changes to OIG’s strategic goals and objectives.

Enterprise Risk Management Benefits OIG

Identifying risks, using risk appetite to prioritize risks, and integrating risk management into corporate processes—all functions of ERM—can help OIG improve organizational decision-making, seize opportunities, and develop and retain a more productive and resilient workforce. When fully implemented, ERM serves as an evidence-based decision-making tool to address OIG’s enterprise-wide risks and includes the following benefits:

- Supports crisis response by mitigating the risks associated with individuals’ altered behavior during a crisis;
- Protects OIG’s reputation;
- Enhances resilience by enabling OIG to respond more rapidly to change;
- Identifies, elevates, and manages risks so the right risks are addressed by the right people at the right time;
- Fosters an organizational culture where risk identification and elevation are encouraged and rewarded;
- Enables line-of-sight into risks across organizational stovepipes to create opportunities to mitigate risks with similar root causes; and

---

5 See Appendix B for OIG’s Strategic Plan Goals and Objectives for Fiscal Years 2019-2022.
6 During a crisis, people’s behavior tends to be emotionally-driven and follows different lines of reasoning than in non-crisis times.
• Leverages knowledge of enterprise risk to improve resource allocation and strategic decision-making.

As OIG’s ERM program evolves and matures, the organization can take advantage of previously unidentified opportunities to improve OIG’s ability to achieve its goals and objectives, enabling OIG to fulfill its oversight mission as fully and efficiently as possible.
OIG’S ENTERPRISE RISK MANAGEMENT APPROACH

Figure 1. Phases of OIG’s Enterprise Risk Management Cycle

1. Establish Context
   Examine both internal and external factors to establish a snapshot of the organizational context at the time of the assessment.

2. Identify Risks
   Before OIG can manage risk, the organization must first identify the risks it faces using a structured and systematic approach.

3. Prioritize Risks
   ERM’s risk analysis process is designed to develop a comprehensive understanding of risks, including potential consequences, current controls, likelihood and severity of risks, and the identification of uncertainties that may aggravate risks. Using the ERM risk analysis process, the Risk Steering Committee will prioritize risks and submit priority recommendations to the Risk Management Council.

4. Identify Strategies for Treatment
   The Risk Management Council will identify strategies for treatment and mitigation of risks and make recommendations to the Inspector General.

5. Respond to Risks
   The Risk Management Council will oversee the assignment of risk owners and the execution of mitigation and corrective action.

6. Monitor and Review
   Risk mitigation activities will be monitored, and following controls testing and review, the Office of ERM will enter a residual risk score into the risk registry.

Continuous Risk Identification and Assessment
The risk identification process is continual. Using data and evidence collection tools such as questionnaires, templates, and surveys, the Office of ERM will continually harvest and analyze risk-related data on existing and emergent risks.

Communication and Consultation
Effective communication is critical to managing enterprise-wide risks. The Office of ERM will work with stakeholders to establish the appropriate risk context, ensure stakeholder perspectives and evidence are effectively incorporated into the risk identification and mitigation process, and strive to advance stakeholder understanding of risk identification and mitigation.

Source: Adapted from OMB Circular No. A-123.
Phases in the Enterprise Risk Management Cycle

OIG’s ERM program employs a six-phase cycle adapted from OMB Circular No. A-123 that integrates risk management into key corporate processes, including strategic planning, performance management, operations, and resource allocation. A summary of this cycle is presented in Figure 1, above. Each phase of OIG’s ERM cycle is described in greater detail below.

Phase 1: Establish Context

Following the adoption of this framework, OIG’s ERM office will analyze internal and external factors to document a snapshot of OIG’s organizational context that will inform subsequent phases of the ERM cycle. This document will discuss scope, methodology, and criteria and address the following topics:

- Legal, cultural, political, regulatory, and financial topics;
- Stakeholder identification and perceptions;
- Policies, procedures, and processes;
- Organizational structure; and
- Decision-making processes.

Phase 2: Identify Risks

Before OIG can manage risk, the organization must first identify the risks it faces using a structured and systematic approach.

Defining Risk

The focus of OIG’s ERM program is on risks that may have an enterprise-wide impact. Enterprise risks are events that have occurred or can potentially occur that would prevent OIG from meeting its mission or achieving its goals and objectives. Examples of enterprise risks include:

- Turnover of key personnel;
- Over-reliance on informal information sharing;
- Failure to follow professional standards;
- Work stoppage due to furlough or unforeseen events (e.g., a pandemic); or
- A change in law affecting OIG’s oversight work.

OIG will use a structured and systematic approach for identifying enterprise risks and populating its risk registry. This approach may include reviewing documentation associated

KEY DEFINITIONS

RISK: the effect of uncertainty on an organization’s ability to meet its objectives

INHERENT RISK: the risk to an entity at the time of the assessment, in the absence of management’s response to the risk

RESIDUAL RISK: the risk that remains after management’s response
with OIG’s past year statements of assurance, conducting interviews with OIG officials representing all component offices, and input from the Risk Steering Committee. OIG employees and contractors are also encouraged to report risks to the ERM office for inclusion in OIG’s risk registry. Unclassified or sensitive but unclassified risks may be emailed to risk@stateoig.gov. Information on classified risks should be emailed to oigriskreporting@state.sgov.gov.

OIG’s ERM program is not a mechanism for resolution of personnel disputes, employee complaints, allegations of discrimination, or criminal matters. Individuals should contact OIG’s Office of the Executive Director (EX) Division of Human Capital (HC) for guidance on where to direct personnel-related complaints and should report instances of criminal activity to the OIG Hotline. Individuals preferring confidentiality or anonymity in reporting risk concerns may also use the OIG Hotline.

Risk Categories and Subcategories

OIG’s enterprise risks can be organized into four main risk categories: strategic, operational, information, and resource management. Each category contains multiple sub-categories of risk that are described below with examples of risks within each subcategory. OIG may refine or introduce additional risk categories and subcategories as its ERM program evolves. Many risks involve multiple categories or subcategories. Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer, and operational consequences for the organization.

<table>
<thead>
<tr>
<th>Strategic Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic risks are internal and external risk factors that can impede OIG’s ability to accomplish its mission, goals, and objectives. These risks may arise internally by pursuing a strategy that is poorly defined or based on flawed or inaccurate data, or from external factors beyond OIG’s control. Risks in this category include changes in the oversight environment, reputational risks, legislation, and management practices at all levels of the organization.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Political</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions or inaction by Congress or the Executive Branch may affect OIG’s ability to perform its mission or achieve its strategic goals and objectives. Examples include:</td>
</tr>
<tr>
<td>• Funding uncertainty or funding cuts</td>
</tr>
<tr>
<td>• Government shutdowns</td>
</tr>
<tr>
<td>• Changes in presidential administrations</td>
</tr>
<tr>
<td>• Changes in Department, USAGM, USIBWC, or OIG senior executive leadership</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks in this subcategory arise from management weaknesses that may affect OIG’s ability to perform its mission or achieve its strategic goals and objectives. Examples include:</td>
</tr>
</tbody>
</table>
- Lack of transparency in decision-making
- Inability to respond and adapt to change or risks
- Failure to foster a culture of inclusiveness
- An organizational culture that does not reflect goals and values
- Inefficient organizational structures

**Compliance**
Compliance risks relate to OIG’s ability to comply with applicable laws, regulations, and professional standards. Examples include:

- Noncompliance with law, regulation, or policy pertaining to human capital management, IT, finance, procurement, or privacy
- Failure to report a potential or actual conflict of interest
- Lack of adherence to professional standards (e.g., Generally Accepted Government Auditing Standards, Quality Standards for Inspections and Evaluations, Quality Standards for Investigations)

**Legal**
Legal risks arise from several sources, such as a defective transaction, a claim being made, or some other legal event that results in a liability or other loss, or a failure to take appropriate measures to meet OIG’s legal or regulatory requirements. Examples include:

- Litigation threats stemming from failure to comply with privacy, records management, or Freedom of Information Act laws and regulations
- Failure to adapt to changes in Federal laws or regulations
- Ethics violations or failures to disclose financial information or external relationships
- Failure to meet court-imposed filing deadlines

**Operational Risks**
Sources of operational risk include inadequate or poorly designed, inefficient, or ineffective internal controls or processes. Such risks may result in fraud, error, impaired customer service, non-compliance, or poor value for money.

**Policies and Procedures**
Risks associated with policies and procedures relate to an inability to provide sufficient guidance and clarification to employees for critical work or core functions. Examples include:

- Outdated policies
- Incomplete, ambiguous, or unclear policies
- Lack of systemic numbering and organization of enterprise-wide policies and procedures

**Contract Management**
Risks associated with contract management relate to contract planning and selection and contractor performance. Examples include:
- Contract management practices that do not comply with law, regulation, or policy
- Violations of the Anti-Deficiency Act and other laws or regulations
- Contractors performing inherently governmental functions
- Contractor use of subcontractors (third-party risks)
- Contractor turnover

### Hazard
Hazard risks arise when employee conduct, organizational attitudes, disruptive events, or lack of awareness and preparation threaten lives and property or hinder efforts to prevent accidents and incidents. Examples include:
- Insider threats or personal crimes, including vandalism
- Terrorist attacks
- Infectious disease outbreaks
- Severe weather events
- Utility failure
- Employees stationed at or traveling to high security risk locations

### Information Risks
Information risks arise from the use of information technology, sharing of information, and reporting of information.

### Technological
Technological risks are associated with the use of technology and its effects on OIG operations. Examples include:
- Noncompliance with the Federal Information Security Modernization Act
- Cybersecurity event or network breach
- Network or server failures
- Inadequate IT resources
- Loss of data
- Lack of data integrity
- Lack of controls to protect classified or personally identifiable information
- Data spillage

### Sharing
Sharing risks are associated with information sharing between and among OIG offices and external stakeholders. Examples include:
- Poor internal communication
- Unauthorized disclosure of closely held information to an external stakeholder
- Inability to obtain required data from the Department, USAGM, or USIBWC
- Failure to adapt messages to intended recipients
- Lack of formal data sharing agreements
- Improper sharing of OIG data and information by third parties

### Reporting
Reporting risks relate to the reliability of OIG’s reporting, including the accuracy and timeliness of reporting needed to support internal decision making, as well as our ability to meet
professional standards, regulations, and stakeholder expectations for information OIG reports externally. Examples include:

- Noncompliance with statutory and regulatory reporting requirements
- Inadequate or inaccurate financial reporting
- Lack of available data to inform strategic decision making
- Failure to complete oversight projects within established timeframes

### Resource Management Risks

Resource management risks arise when OIG’s management of key business processes affect the reliability, timeliness, effectiveness, or quality of OIG’s work.

### Human Capital

Human capital risks arise from mismanagement of the workforce, the unavailability of sufficient capacity and capability, non-compliance with relevant employment law, regulation or policy, lack of adherence to Merit System principles, instances where the demand for necessary skills drives salaries above the available federal salary cap, and real or perceived inequities. Examples include:

- Slow or poorly managed hiring and security processes
- Failure to hire and retain talent
- Failure to recruit and retain a diverse workforce
- Insufficient or inadequate professional development or training
- Inequitable awards distribution
- Abuse of personnel benefits

### Physical Assets

Physical asset risks arise when facilities, equipment, or personal property deemed significant enough to track, inventory, and monitor, are not sufficiently tracked, inventoried, and monitored. Examples include:

- Failure to properly inventory or track personal property
- Failure to protect and preserve investigative evidence

### Financial Management

Financial management risks relate to budget planning and execution activities, including the execution of congressional appropriations, accuracy of financial reporting, and compliance with relevant laws. Examples include:

- Lack of transparency in budget planning and execution
- Failure to align resources with strategic priorities
- Failure to ensure separation of duties
- Misuse of purchase or travel cards
- Wasteful or unnecessary expenditures
Phase 3: Prioritize Risks

The result of the risk identification and categorization process is a comprehensive inventory of risks. OIG will consider the root cause, source(s), probability of occurrence, and potential positive or negative outcomes for each identified risk. Such an analysis allows OIG to prioritize the identified risks. The ERM office will perform a likelihood and impact analysis, which will include potential consequences for identified risks, existing controls, and identification of uncertainties. Based on this analysis, risks will be assigned separate impact and likelihood scores, using the scale outlined in Figure 2, below. The impact and likelihood scores will be averaged to obtain an inherent risk score. The inherent risk score measures the risk at the time of assessment before any action is taken to manage it beyond normal operations. The ERM office will also assign a residual risk score, which is the average of the impact and likelihood scores after management’s response to a given risk.

Figure 2. Risk Scoring Scale

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Very High</strong> (5)</td>
<td></td>
</tr>
<tr>
<td>Degradation of an activity or role is severe and affects our ability to meet one or more strategic goals or objectives, produce key deliverables, or reach required levels of performance to meet the mission.</td>
<td>Certain (5)</td>
</tr>
<tr>
<td></td>
<td>Likelihood of occurrence is 90 – 100 percent.</td>
</tr>
<tr>
<td><strong>High</strong> (4)</td>
<td></td>
</tr>
<tr>
<td>Degradation of an activity or role is major, requiring immediate escalation or management intervention to reach required levels of performance of key functions.</td>
<td>Likely (4)</td>
</tr>
<tr>
<td></td>
<td>Likelihood of occurrence is 50 – 90 percent.</td>
</tr>
<tr>
<td><strong>Moderate</strong> (3)</td>
<td></td>
</tr>
<tr>
<td>Degradation of an activity or role is moderate, with material impact on performance of key functions.</td>
<td>Possible (3)</td>
</tr>
<tr>
<td></td>
<td>Likelihood of occurrence is 25 – 49 percent.</td>
</tr>
<tr>
<td><strong>Low</strong> (2)</td>
<td></td>
</tr>
<tr>
<td>Degradation of an activity or role is minor. It is noticeable and may affect performance of key functions.</td>
<td>Unlikely (2)</td>
</tr>
<tr>
<td></td>
<td>Likelihood of occurrence is 10 – 24 percent.</td>
</tr>
<tr>
<td><strong>Very Low</strong> (1)</td>
<td></td>
</tr>
<tr>
<td>Degradation in activity or role is negligible and is not expected to significantly affect performance of key functions.</td>
<td>Remote (1)</td>
</tr>
<tr>
<td></td>
<td>Likelihood of occurrence is 0 – 9 percent.</td>
</tr>
</tbody>
</table>


The result of the risk analysis and evaluation process will be the creation of a risk profile, a prioritized inventory of the most significant risks identified in the risk assessment process.
Consistent with the requirements of OMB Circular No. A-123, OIG’s risk profile will include an evaluation of fraud risks and use a risk-based approach to design and implement financial and administrative control activities to mitigate any identified material fraud risks. The risk profile will include the following elements:

- Strategic goals and objectives affected by the risk;
- Definition of the risk;
- Inherent risk assessment;
- Current risk response strategies;
- Residual risk assessment;
- Proposed risk response, including monitoring activities; and
- Proposed mitigation plan.

Phase 4: Identify Strategies for Treatment

Once risks are prioritized, OIG will identify and assess the range of response options or strategies to tolerate, transfer, terminate, or treat the organization’s most important risks. Possible risk treatment options are outlined in Figure 3, below. The ERM office will provide risk analysis documentation to OIG’s Risk Steering Committee (RSC) to assist in determining which risks the RSC will send to the Risk Management Council (RMC) for treatment consideration.

The RSC, comprised of OIG employees at or below the GS-15 level or equivalent, represent the interests of their respective offices by communicating their office’s ERM activity and needs. The RMC, chaired by the Deputy Inspector General or a designee, comprises OIG senior leaders who are responsible for managing risks within their respective program areas and, based on inputs from the RSC, will consider the enterprise-wide implications of proposed risk treatments and make risk treatment recommendations to the Inspector General (IG) for final approval. The governance of OIG’s ERM program, including the functions of the RSC and RMC, is described below.

Figure 3. Risk Treatment Options

<table>
<thead>
<tr>
<th>Tolerate</th>
<th>The risk exposure is considered tolerable, requiring no further action.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer</td>
<td>Delegate risk by entering agreements with independent third parties to outsource processes or activities through contractual arrangements.</td>
</tr>
<tr>
<td>Terminate</td>
<td>The risk exposure is not considered tolerable. Termination will discontinue operations or activities; prohibit unacceptably high-risk activities and process exposures through appropriate policies and procedures; or stop specific activities by redefining objectives, refocusing strategic plans and policies, or redirecting resources.</td>
</tr>
</tbody>
</table>
By selecting treatment, the RMC has decided to continue with the activity, with specific actions being taken to lower risk to an acceptable level. The treatment options can be organized into four types of controls:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive Controls</td>
<td>These controls are designed to limit the possibility of an undesirable outcome being realized.</td>
</tr>
<tr>
<td>Corrective Controls</td>
<td>These controls are designed to correct undesirable outcomes which have occurred.</td>
</tr>
<tr>
<td>Directive Controls</td>
<td>These controls are designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided, typically associated with health, safety, or security.</td>
</tr>
</tbody>
</table>
| Detective Controls | These controls are designed to identify when undesirable outcomes have occurred. Their effect is, by definition, “after the event,” so they are only appropriate when it is possible to accept the loss or damage incurred. Examples of detective controls include:  
  - Asset checks to detect whether assets have been removed without authorization.  
  - Reconciliation to detect unauthorized transactions.  
  - “Post Implementation Reviews” to detect lessons to be learned from projects for application in future work.  
  - Monitoring activities to detect changes that should be addressed. |

Source: OIG.

**Phase 5: Respond to Risks**

The IG will make final determinations regarding OIG’s treatment of enterprise risks, including how finite human and financial resources are to be allocated to treat identified risks. An office within OIG will be designated the risk owner and will oversee the implementation of an approved treatment action plan. The ERM office will notify assistant inspectors general (AIGs) or their equivalents when their office has been designated as a risk owner by the IG and request that they assign an accountable party in their office to draft the risk treatment plan and to oversee its implementation.

**Phase 6: Monitor and Review**

OIG will monitor and review the organization’s risk responses and mitigations on a regular basis. Risk owners will provide the ERM office quarterly updates on progress toward completing the risk treatment plan. OIG’s Office of the Executive Director (EX) Division of Operational Controls and Compliance (OCC) will advise on planning, performing, reporting on
controls testing, and documenting mitigation and corrective action, consistent with its responsibilities related to OIG’s annual statement of assurance process. Risk owners will test the effectiveness of implemented controls within 6 months of completing a risk treatment plan. After a risk is treated, the ERM office will assign a residual risk score in OIG’s risk registry.

*Continuous Risk Identification and Assessment*

Identifying risks must be an iterative process. The ERM Office will continually identify and analyze risk-related data to identify new risks or changes to existing risks.

**Figure 4. OIG’s Enterprise Risk Management Governance Process**

*ERM Office*
The office conducts an enterprise-wide threshold risk review, inclusive of impact and likelihood analysis to prioritize risks, and provides a contextual-based risk map to RSC.

*IG*
The IG will make a final determination on risk treatment. As appropriate, the IG designates a risk owner, typically an AIG, who will oversee the implementation of an approved treatment action plan.

*RSC*
Using the ERM office’s risk documentation, the RSC conducts a second-tier analysis to determine which risks to send to the RMC for review and resolution.

*RMC*
Under the risk treatment rubric outlined in this Framework, on a quarterly basis the RMC will review risks, ultimately deciding which treatment recommendations to recommend to the IG.

*AIG/Risk Owner*
The risk owner selects an accountable party in their office, such as a division director or Special Agent in Charge, to oversee the implementation of a treatment action plan.

*Accountable Party*
The accountable party provides ERM with quarterly updates on progress toward completing the risk treatment action plan.

*Risk Owner and EX/OCC*
Risk owners test the effectiveness of implemented controls after completing a risk treatment plan. As part of the Statement of Assurance process, EX/OCC analyzes planned corrective actions to determine whether they have been effectively completed and whether risk mitigation was effective.

*ERM Office*
Based on the results of mitigation or corrective action, ERM will enter a residual risk score in the risk registry.

Source: OIG.
Governance of OIG’s Enterprise Risk Management Program

Multiple OIG stakeholders are involved in the implementation of OIG’s ERM program. The governance model described in this framework is guided by requirements outlined in OMB Circular No. A-123, as well as best practices employed by other Federal agencies that have established ERM programs. This framework empowers two bodies—the RMC and RSC—to inform the IG’s decision-making on enterprise risks. The RMC and RSC will work together to ensure that OIG employees and contractors at every level have opportunities to identify risks and that OIG identifies and takes action to address the organization’s most important risks. In addition to these newly created bodies, OIG’s existing offices will continue to play important roles related to risk management and internal control. OIG’s ERM governance process is summarized in Figure 4, above.

Enterprise Risk Management Roles and Responsibilities

To ensure the successful implementation of OIG’s ERM program, this framework defines roles and responsibilities for OIG stakeholders responsible for identifying and responding to enterprise-wide risks. The roles and responsibilities, described below, relate to the phases of OIG’s ERM cycle previously described.

Inspector General

The IG is responsible for all OIG functions, including the organization’s responsibilities related to ERM and internal control. The IG, in conjunction with the RMC, sets the tone at the top to build and sustain commitment to ERM principles and practices at all levels of the organization. Based on recommendations from the RMC, the IG makes decisions on risk treatment, designates a risk owner for specific risks, and makes related resource allocation decisions.

Risk Steering Committee

The RSC is comprised of OIG employees at or below the GS-15 level or equivalent. The RSC will initially be comprised of at least one risk champion from each OIG office to serve for a term of at least 1 year. Members of the RSC represent the interests of their respective offices by communicating their office’s ERM activity and needs. The ERM office organizes and facilitates meetings of the RSC. Specific duties of the RSC are outlined in the RSC charter.

Risk Management Council

The RMC is chaired by the Deputy Inspector General or a designee. In addition to the Deputy Inspector General, members of the RMC include:

- Chief of Staff
- AIGs or their designees
- General Counsel
- Executive Director
- Chief Information Officer
• Director of Organizational Health
• Director of Congressional and Public Affairs
• Director of ERM

RMC members are responsible for managing risks within their respective program areas and, based on inputs from the RSC, making recommendations to the IG concerning risk issues and treatment. Specific duties of the RMC are outlined in the RMC charter.

Assistant Inspectors General

AIGs are responsible for overseeing the implementation of risk treatments for which their office is designated the risk owner. The AIGs or their designee will participate in meetings of the RMC. AIGs will assign an accountable party in their respective office to draft the risk treatment plan and to oversee its implementation. AIGs will also ensure the submission of quarterly updates to the ERM office. These updates will outline risk treatments for which they have responsibility and ensure that implemented controls are tested for effectiveness within 6 months of completion.

Office of Enterprise Risk Management

The Director of ERM, under the supervision of OIG’s Chief of Staff, manages OIG’s ERM program and encourages a risk-aware culture that promotes accountability at all levels of the organization. The ERM office supports and facilitates the activities of the RMC and RSC. The office also advises and trains OIG employees and contractors on ERM principles, tools, and strategies; identifies trends and drivers of change and uncertainty that can affect OIG’s ability to meet its mission; and coordinates OIG’s ERM program activity and advances the program’s maturity.

Office of Operational Controls and Compliance

EX/OCC leads OIG’s annual Statement of Assurance process, including review of recommended internal controls testing by offices and the collection and review of internal control testing results. EX/OCC performs independent internal control reviews based on priority and compliance risks. EX/OCC also independently analyzes planned corrective actions to determine whether, if implemented, the risk mitigation would be effective. As OIG’s ERM program matures, EX/OCC will work in coordination with the ERM office to integrate the organization’s ERM and internal controls functions.

All OIG Employees

All OIG employees and contractors are encouraged to report risks directly to the ERM office or through their office’s representative(s) on the RSC. All OIG employees have a responsibility to speak candidly and escalate risk-related concerns to management and may do so without fear of reprisal. If an OIG employee prefers confidentiality or anonymity, the employee may report risk concerns via the OIG Hotline.
ENTERPRISE RISK MANAGEMENT PROGRAM MATURITY

In January 2018, OIG established a dedicated ERM office after the then-Inspector General determined that doing so would be beneficial to OIG’s efforts to assess risk and improve oversight of the Department, USAGM, and USIBWC. In May 2018, OIG published its first ERM Strategic Framework. This updated framework reflects work performed by the ERM office to date, including dozens of risk interviews with OIG employees and initial population of the organization’s risk registry.

**ERM Maturity and Assessment Model**

OMB’s Circular No. A-123 advises agencies to develop a maturity model approach to the adoption of an ERM framework. ERM programs typically start informally and gain sophistication and capacity over time. This concept is called ERM maturity. As the value and usefulness of an ERM becomes apparent and associated processes are institutionalized, the program progresses and matures. OIG has adopted OMB’s Federal ERM Maturity Model. As described in Appendix C, the model considers five attributes for assessing maturation: program attributes, key practices, risk culture, organizational benefits, and executive engagement. OIG’s ERM office performed a self-assessment identifying where OIG falls on the maturity model as of the fourth quarter of FY 2021, and where it aspires to be 18 months following the publication of this framework. In the office’s assessment, OIG’s ERM current maturity level falls between “initial ad hoc” and “fragmented early stages”—that is, between levels 1 and level 2 in the OMB model. The ERM office recommends that OIG strive to reach a level of “defined coordinated” (level 3) by the end of FY 2023. The ERM office will solicit annual stakeholder feedback as part of OIG’s ERM maturity assessment process going forward.
APPENDIX A: OIG VISION, MISSION, AND VALUES

OUR VISION
To be a world-class organization and a catalyst for effective management, accountability, and positive change in the Department, the U.S. Agency for Global Media, and the foreign affairs community.

OUR MISSION
To conduct independent audits, inspections, evaluations, and investigations to promote economy and efficiency and to prevent and detect waste, fraud, abuse, and mismanagement in the programs and operations of the Department and the U.S. Agency for Global Media.

OUR VALUES

ACCOUNTABILITY
We accept responsibility for our work products, services, and performance.

RESPECT
We promote diversity in the workplace and treat people with dignity and respect. We expect civility as we conduct our work and in our interactions with each other.

COMMUNICATION
We clarify expectations and encourage candor. We communicate with purpose and strive to align our words and our actions and to be aware of the effect we have on others. We look for ways to improve ourselves and our work by expressing appreciation and by giving and accepting constructive feedback.

TEAMWORK
We foster a diverse, inclusive, collaborative, and trusting culture where people can share their ideas and opinions. We empower and engage our colleagues to achieve outstanding organizational results.

INTEGRITY
We maintain our independence and act with courage, honesty, and professionalism. Our work is fact-based, objective, and supported by sufficient evidence that meets professional standards.

CURIOSITY
We are committed to learning about and listening to others’ perspectives, objectives, and challenges. We seek new information to inspire creative and analytical thinking. We foster an environment that fuels innovation and results.
## APPENDIX B: OIG STRATEGIC PLAN GOALS AND OBJECTIVES FOR FYs 2019-2022

### STRATEGIC GOAL 1
**To serve the American people and support the Department and USAGM, we advance fiscal responsibility and accountability**

<table>
<thead>
<tr>
<th>OBJECTIVE 1.1</th>
<th>OBJECTIVE 1.2</th>
<th>OBJECTIVE 1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct OIG resources to high and emerging risks, priority areas, and the identification of cost savings</td>
<td>Drive the timely completion of OIG products</td>
<td>Drive implementation of OIG recommendations</td>
</tr>
</tbody>
</table>

### STRATEGIC GOAL 2
**In support of Department and other USG personnel, we strengthen the Department’s ability to protect people, information, and facilities**

<table>
<thead>
<tr>
<th>OBJECTIVE 2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strengthen Department and USAGM security, information technology, and safety programs and operations by identifying risks and improving adherence to standards</td>
</tr>
</tbody>
</table>

### STRATEGIC GOAL 3
**On behalf of the American people, we advance efficiency and transparency of OIG’s oversight mission**

<table>
<thead>
<tr>
<th>OBJECTIVE 3.1</th>
<th>OBJECTIVE 3.2</th>
<th>OBJECTIVE 3.3</th>
<th>OBJECTIVE 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strengthen OIG’s use of resources through strategic planning improvements and the expansion of enterprise risk management</td>
<td>Leverage strategic communications to expand outreach to our stakeholders</td>
<td>Enhance OIG’s use of technology to improve organizational efficiency and achievements</td>
<td>Enhance the timeliness, quality, and customer experience of OIG mission support activities</td>
</tr>
</tbody>
</table>

### STRATEGIC GOAL 4
**To support our staff, we foster a diverse and inclusive culture that inspires innovation, high performance, engagement, and accountability**

<table>
<thead>
<tr>
<th>OBJECTIVE 4.1</th>
<th>OBJECTIVE 4.2</th>
<th>OBJECTIVE 4.3</th>
<th>OBJECTIVE 4.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cultivate a culture of inclusiveness at all levels by fostering a fair, open, diverse, and cooperative working environment</td>
<td>Provide opportunities for continuous development and professional growth to meet current and future OIG mission needs</td>
<td>Advance strategic recruitment, succession, and retention planning</td>
<td>Increase leadership and management effectiveness</td>
</tr>
</tbody>
</table>
APPENDIX C: ENTERPRISE RISK MANAGEMENT MATURITY MODEL

The Office of Management and Budget’s (OMB) Federal Enterprise Risk Management (ERM) Maturity Model is used to gauge an ERM program’s advancement along a defined spectrum. OMB designed the model to be used by all Federal agencies. The model is used primarily to self-identify an ERM program’s maturity and identify steps to move the program toward maturity. The model will evolve as more data points become available to identify a program’s maturity level. OIG’s ERM office will update its maturity model in future framework releases to incorporate developments in OMB’s maturity model.

ERM program maturity is rated on a five-point scale:

- Level 1: Initial Ad-hoc
- Level 2: Fragmented Early Stages
- Level 3: Defined Coordinated
- Level 4: Institutionalized Instilled
- Level 5: Optimized Predictive

Each level includes five qualities: program attributes, key practices, risk culture, organizational benefits, and executive engagement. The ERM office uses these qualities to perform a self-assessment to determine OIG’s current maturity level and to identify actions that will allow OIG’s ERM program to advance to the next level of maturity.

<table>
<thead>
<tr>
<th>Level 1: Initial Ad-hoc</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Program Attributes</strong></td>
</tr>
<tr>
<td>No formal cross-cutting ERM governance</td>
</tr>
<tr>
<td>Decentralized roles/responsibilities</td>
</tr>
<tr>
<td>Isolated risk management processes</td>
</tr>
<tr>
<td>Transactional</td>
</tr>
<tr>
<td><strong>Key Practices</strong></td>
</tr>
<tr>
<td>Intermittent</td>
</tr>
<tr>
<td>Few activities defined</td>
</tr>
<tr>
<td>Quick-fix risk management</td>
</tr>
<tr>
<td><strong>Organizational Benefits</strong></td>
</tr>
<tr>
<td>Unaware of the value of ERM</td>
</tr>
<tr>
<td>Organization is not defined</td>
</tr>
<tr>
<td><strong>Risk Culture</strong></td>
</tr>
<tr>
<td>Risk responses are reactive</td>
</tr>
<tr>
<td>Backward looking</td>
</tr>
<tr>
<td>Unpredictable</td>
</tr>
<tr>
<td>Minimal capacity to respond efficiently and effectively</td>
</tr>
<tr>
<td>Cooperative engagement with oversight entities</td>
</tr>
<tr>
<td>Provides information and data to oversight entities (compliance driven)</td>
</tr>
<tr>
<td>Considers risk intelligence provided by oversight entities</td>
</tr>
<tr>
<td><strong>Executive Engagement</strong></td>
</tr>
<tr>
<td>Ad-hoc</td>
</tr>
<tr>
<td>Haphazard feedback</td>
</tr>
<tr>
<td>Informal (impromptu) input</td>
</tr>
</tbody>
</table>

### Level 2: Fragmented Early Stages

**Program Attributes**
- Some enterprise governance
- Some ERM responsibilities built into existing roles
- Tactical
- Agency enterprise goals or objectives considered

**Key Practices**
- Emerging enterprise risk management discipline
- Risks managed in siloes (localized experiences/processes)
- Disparate monitoring/reporting
- Inconsistent risk definitions

**Organizational Benefits**
- Independent risk activities
- Low perceived value to mission
- Compliance driven

**Risk Culture**
- Risk responses are functional, reactive problem solving
- Risk management for short-term benefits
- Minimally predictive
- Cooperative engagement with oversight entities
- Provides information and data to oversight entities (engagement-driven)
- Considers risk intelligence provided by oversight entities

**Executive Engagement**
- Some management involvement when risk issues are reported
- Limited understanding of ERM and risk awareness

### Level 3: Defined Coordinated

**Program Attributes**
- Formally established roles and responsibilities
- Formal enterprise governance exists
- Some knowledge sharing across risk functions

**Key Practices**
- Standardized ERM program and practices are documented
- ERM processes evolving but not fully integrated
- Enterprise risk measured/managed primarily qualitatively
- Enterprise risk information is routinely and consistently monitored and reported to support prioritization
- Introduction of risk appetite

**Organizational Benefits**
- Moderate perceived value to mission
- Informs priorities for risk-based decision making

**Risk Culture**
- Risk responses are focused on prevention
- Action plans implemented in response to high priority risks
- Collaborative engagement with oversight entities
- Engages and shares risk information with oversight entities
- Receptive to risk intelligence provided by oversight entities

**Executive Engagement**
- Strategically reviewing top enterprise risk
- Actively promoting an open risk dialogue
- Familiarity with and initial training in ERM
Level 4: Institutionalized Instilled

**Program Attributes**
- Identify opportunities for informed risk taking
- Coordinated risk management activities across identified segments
- Identify and document enterprise risk/reward tradeoff
- Enterprise governance considers risk during strategic goal setting and resource allocation

**Key Practices**
- Instilled ERM discipline
- Fully standardized ERM processes integrated with tools and data
- Enterprise risk measured quantitatively/qualitatively with interdependencies identified
- Define risk appetite and tolerances

**Organizational Benefits**
- Preventing issues and creating value
- Readily adaptable to mission/organizational change (external)
- Informed risk taking aligned with enterprise strategy
- High perceived value to mission

**Risk Culture**
- Risk response is proactive and predictable
- Processes are monitored and reviewed for continuous improvement
- Open and inclusive environment and staff are encouraged to discuss risks internally
- Highly collaborative engagement with oversight entities
- Actively engages and regularly shares risk information with oversight entities
- Requests/seeks additional risk intelligence from oversight entities

**Executive Engagement**
- Executive ownership at enterprise level
- Risk discussions considered in strategic planning and resource allocation
- Decision making based on risk reward and tradeoff issues
- Engaging in ERM open dialogue

Level 5: Optimized Predictive

**Program Attributes**
- Provides platform for enterprise agility and innovation
- Leverage opportunities for informed risk taking and strategic planning
- Leverage internal/external horizon scanning to identify emerging risks
- Continuous improvement methods used to prepare for future
- ERM program facilitates knowledge sharing

**Key Practices**
- Integrated external data sources that enhance insight
- Risk modeling/scenarios applied
- Risk appetite and tolerance clearly understood with alerts in place when thresholds are exceeded
- Recognized as best in class

**Organizational Benefits**
- Resilient and agile enterprise built to pivot and respond to opportunity and change

**Risk Culture**
- Extended enterprise embedded in strategic planning and decision making
- Transformational value to mission

**Executive Engagement**
- Risk response is anticipatory
- Stakeholders believe that risk management is everyone’s job and there is an open environment that fosters objective discussions about risk across the enterprise
- Oversight entities are valued partners
- Proactively engages and shares risk information with oversight entities
- Regularly requests and integrates risk intelligence provided by oversight entities

**Executive Engagement**
- Risk-sensing discussions embedded in strategic planning and resource allocation
- External and internal executive champions align mission delivery to strategic objectives
- Engaging in sustained open dialogue