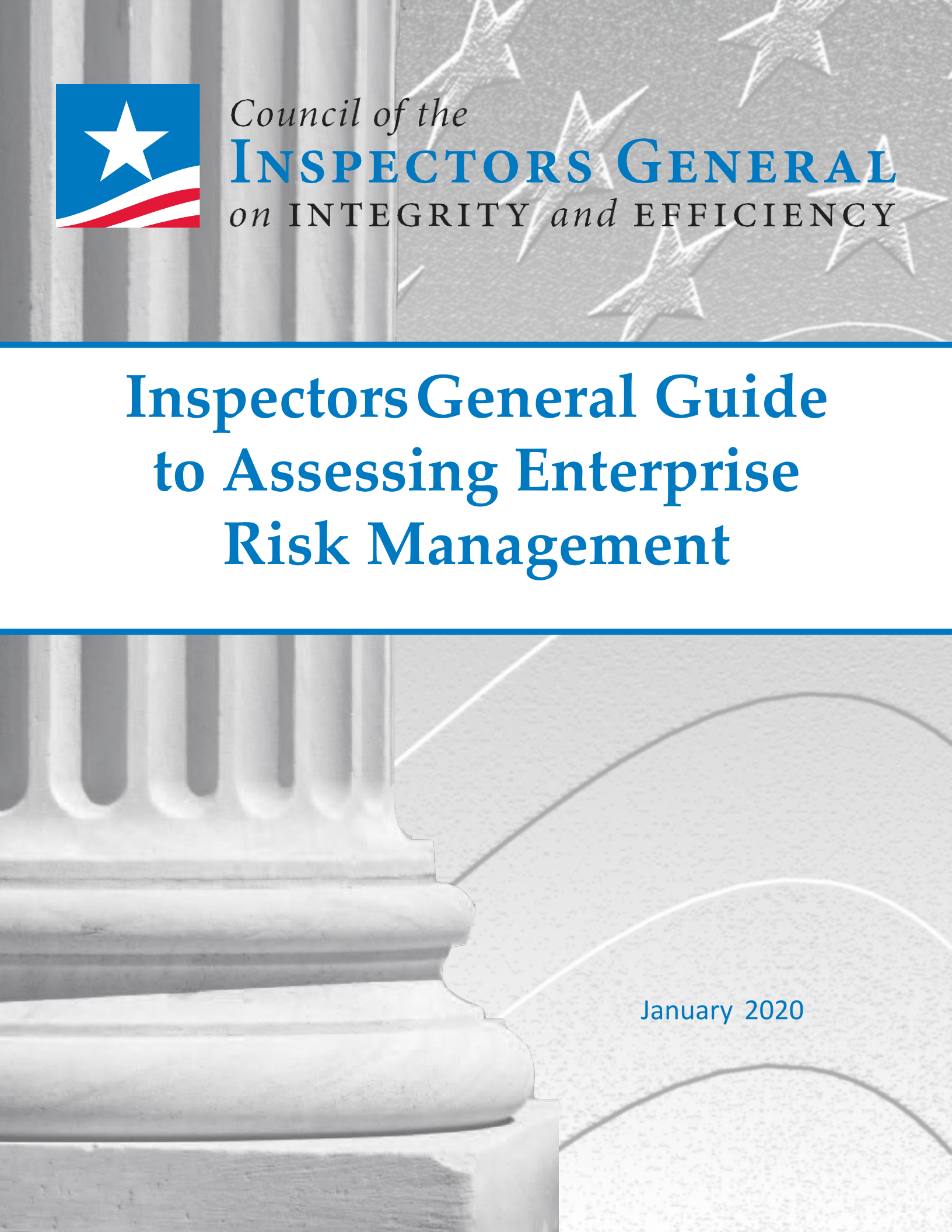


Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

Inspectors General Guide to Assessing Enterprise Risk Management

January 2020

EXECUTIVE SUMMARY

Objective

The purpose of the *Inspectors General Guide to Assessing Enterprise Risk Management* is to provide Federal Offices of Inspectors General (OIG) with information useful for assessing—either auditing or evaluating in accordance with applicable professional standards—the enterprise risk management (ERM) programs at their component agencies.

Approach

To accomplish this objective, personnel from various OIGs and the Office of Management and Budget (OMB) worked together throughout 2018 and 2019 to identify and compile information on relevant criteria, good ERM practices, prior reviews, and training resources. The resulting guide was subject to extensive peer review, including input from various executive branch ERM practitioners, to ensure accuracy, completeness, and readability. As Federal ERM requirements, guidance, and best practices evolve, this guide may be updated.

On July 15, 2016, OMB issued its revised Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB Circular No. A-123), which established various ERM processes in the Federal Government. As defined by the Circular, ERM is "an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos."

OMB Circular No. A-123 requires agencies to implement an ERM capability coordinated with the strategic planning and strategic review process established by the Government Performance and Results Modernization Act of 2010 (Pub. L. No. 111-352), and the internal control processes required by the Federal Managers' Financial Integrity Act of 1982 (Pub. L. No. 97-255), and the Government Accountability Office's *Standards for Internal Control in the Federal Government* (the "Green Book"). Moreover, OMB Circular No. A-123 states that agency managers and Inspectors General should establish "a new set of parameters encouraging the free flow of information about agency risk points and corrective measure adoption," resulting in the earlier identification of risk, allowing the opportunity to develop a collaborative response, and leading to a more resilient government.

In 2017, the Council of the Inspectors General on Integrity and Efficiency established the ERM Working Group to contribute to the promotion and implementation of ERM principles within the OIG community. A sub-group of the ERM Working Group wrote this guide to provide OIGs with information on relevant criteria, good practices, and prior Federal Government ERM reviews. In addition, Exhibit A offers possible steps for OIGs to consider when developing plans to assess agency ERM programs. Finally, Exhibit B provides information on ERM-related training resources available as of January 2020 to help OIGs gain the knowledge necessary to assess agency ERM programs.

TABLE OF CONTENTS

BACKGROUND AND OBJECTIVE

Background

According to the IBM Center for the Business of Government, historically, the Federal sector lacked a standard risk management methodology and "…organizations focused on hazard risk management and insurable financial risks."[1] The U.S. Government Accountability Office (GAO) first issued its risk management framework in 2005 related to homeland security efforts for assessing threats and taking appropriate steps to deal with them.[2] At that time, there was no established universally agreed-upon set of requirements or processes for a risk management framework specifically related to homeland security and combating terrorism. Nonetheless, even before the issuance of Government-wide enterprise risk management (ERM) requirements in 2016, GAO reported that several agencies were implementing ERM to address risk-based issues and improve their ability to respond to future risks. For example:

- In 2004, the Office of Federal Student Aid in the U.S. Department of Education adopted ERM, in part, to help address longstanding risks including poor financial management and internal controls.

- In 2013, the Internal Revenue Service (IRS) adopted an ERM program to address issues related to reviewing tax-exempt applications and broadly improving operations.

- In 2014, the Office of Public and Indian Housing at the Department of Housing and Urban Development finalized its ERM framework and implementation plans in response to several high profile financial and compliance issues with public housing authorities, among other concerns related to its internal controls and risk management practices.[3]

On July 15, 2016, the Office of Management and Budget (OMB) issued its revised Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB Circular No. A-123), which established various ERM processes in the Federal Government. As defined by the Circular, ERM is "an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos." OMB Circular No. A-123 further states that "ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery." Moreover, ERM reflects "forward-looking management decisions and balancing risks

[1] IBM Center for the Business of Government, *Managing Risk in Government: An Introduction to Enterprise Risk Management*, Dr. Karen Hardy; Financial Management Series, 2010 Second Edition. Hazards may include, but not be limited to, liability, theft, and fire.

[2] U.S. Government Accountability Office, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Critical Infrastructure* (GAO-06-91; December 15, 2005).

[3] U.S. Government Accountability Office, *Selected Agencies' Experiences Illustrate Good Practices in Managing Risk* (GAO-17-63; December 1, 2016).

and returns so an Agency enhances its value to the taxpayer and increases its ability to achieve its strategic objectives."

OMB Circular No. A-123 requires agencies to implement an ERM capability coordinated with the strategic planning and strategic review process established by the Government Performance and Results Modernization Act of 2010 (GPRAMA),[4] and the internal control processes required by the Federal Managers' Financial Integrity Act of 1982 (FMFIA)[5] and GAO's *Standards for Internal Control in the Federal Government* (the "Green Book," discussed further on page 8).[6] GPRAMA requires agencies to engage in performance management tasks such as setting goals, measuring results, and reporting progress. FMFIA requires agencies to establish internal control and financial systems that provide reasonable assurance of achieving the three objectives of internal control: (1) effectiveness and efficiency of operations, (2) compliance with regulations and applicable laws, and (3) reliability of financial reporting. Finally, the Green Book sets the standards for an effective internal control system for Federal agencies and provides the overall framework for designing, implementing, and operating an effective internal control system. As Figure 1 shows, internal controls are an integral part of risk management and ERM.

Figure 1. The Relationship Between Internal Controls and ERM

Source: OMB Circular No. A-123.

[4] Pub. L. No. 111-352, 124 Stat. 3866 (2011). GPRAMA amends the Government Performance and Results Act of 1993, Pub. L. No. 103-62, 107 Stat. 285 (1993).

[5] Pub. L. No. 97-255, 96 Stat. 814 (1982).

[6] U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G; September 2014).

Role of Agency Management in ERM

Agency management is responsible for implementing practices that effectively identify, assess, respond to, and report on risks. To do this, agencies must incorporate risk awareness into the agencies' culture and ways of doing business. According to OMB Circular No. A-123, successful implementation of the Circular requires agencies to "establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame." In implementing an ERM program, it is management's responsibility to:

- determine the comprehensiveness and granularity of the risk profile and risk inventory;
- determine which risks should be captured in the risk inventory and summarized in the risk profile; and
- prioritize risks based on the likelihood and impact of the risk occurring, and deciding the appropriate risk response.

Among other sources of information, management uses the results of Office of Inspector General (OIG) reviews, including accompanying findings and recommendations, to monitor the design or operating effectiveness of its ERM program.

Role of OIG in ERM

As set forth in the Inspector General Act of 1978 (the IG Act), as amended, OIGs conduct independent and objective audits and investigations of agency programs and operations.[7] Such work may include reviewing aspects of internal control and risk management. Among other things, OIGs are also responsible for keeping management informed about risks they detect, including fraud risks, and providing information to management for use in identifying and assessing risks. In particular, OMB Circular No. A-123 encourages an "open and transparent culture" in an effort to support "the earlier identification of risk . . . leading to a more resilient government." To this end, in accordance with Section 6 of the IG Act, each Inspector General is authorized to have, among other things, "timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials available" that relate to the OIG's responsibilities established under the Act.

When designing approaches and steps to assess an agency's ERM program, OIG auditors and evaluators should consider the following:

- ERM has the potential to be a helpful management tool. Through independent and objective audits and evaluations, OIGs can assist agencies in developing more mature and capable ERM programs. One way to accomplish this goal is to focus audits and evaluations on agencies' risk management processes.

[7] Pub. L. No. 95–452, 92 Stat. 1101 (1978).

- According to OMB Circular No. A-123, agency risk profiles will often contain pre-decisional, deliberative, confidential, or sensitive information. Moreover, their development requires candor, subjective evaluations, and frank discussions. Nonetheless, the Circular encourages the "free flow of information" about agency risks and corrective measures.

- OMB Circular No. A-123 provides agencies with flexibility in how to implement ERM, including the format and content of the agency risk profile.

- Consistent with GAO's *Government Auditing Standards*[8] and the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation*,[9] assuming management responsibilities and making or approving business risk decisions is an impairment to auditor/evaluator independence.

Objective

In 2017, CIGIE established the ERM Working Group to contribute to the promotion and implementation of ERM principles within the OIG community. A sub-group of the ERM Working Group, comprised of personnel from various OIGs and OMB, worked together throughout 2018 and 2019 to write this guide. The objective of this guide is to provide Federal OIGs with information useful for assessing—either auditing or evaluating in accordance with applicable professional standards—the ERM programs at their component agencies. Although this guide provides the OIG community with a baseline framework for assessing ERM programs, there is no one-size-fits-all approach toward ERM. ERM is an iterative process and each agency operates in a unique environment. Therefore, steps (and to some extent criteria) for assessing agency ERM programs may vary among OIGs. When planning to assess an agency's ERM program, OIGs should gain and document an understanding of the agency's risk management procedures, risk framework, and risk maturity model.[10] In addition, auditors and evaluators should use professional judgment to develop steps based on various factors, including:

- the size of the assessed entity;

- where the entity is in the ERM implementation process (that is, its maturity); and

- the process the entity uses to document and communicate risks.

As Federal ERM requirements, guidance, and best practices evolve, this guide may be updated.

[8] U.S. Government Accountability Office, *Government Auditing Standards* (GAO-18-568G 3.106; 2018 Revision).

[9] Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation* (Independence Standard; January 2012).

[10] OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (July 2016), defines "risk" as the effect of uncertainty on objectives.

RELEVANT CRITERIA, GOOD PRACTICES, AND OTHER RESOURCES

OMB Circular No. A-123

In addition to agency policies and procedures and any other agency-specific criteria, OIGs should familiarize themselves with OMB Circular No. A-123, which is applicable to each executive agency[11] (non-executive agencies of the Federal Government are encouraged to adopt the Circular) and provides specific requirements for assessing and reporting on controls in the Federal Government. The Circular outlines the following required ERM activities:

- Governance
- Risk Profiles
- Implementation

A summary of the requirements associated with each of these activities, as described in OMB Circular No. A-123, is provided below.

Governance. Management should establish a governance structure to effectively implement, direct, and oversee implementation of OMB Circular No. A-123 and all the provisions of a robust process of risk management and internal control. The responsibilities of managing risks are shared throughout the agency from the highest levels of executive leadership to the service delivery staff executing Federal programs. Agency governance should include a process that considers the following characteristics identified in industry best practices:

- developing and implementing core policies and procedures with respect to ERM, including a process to define risk appetite[12] and establish risk tolerance,[13] accordingly;
- ensuring the current risk levels and processes are consistent with the established risk tolerance and policies;
- supporting implementation of effective controls;

[11] There are 15 executive agencies that are the primary units of the executive branch of the Federal Government of the United States. The list of the agencies can be found at *https://www.usa.gov/executive-departments*.

[12] OMB Circular No. A-123 defines "risk appetite" as 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 to set strategy and select objectives.

[13] OMB Circular No. A-123 defines "risk tolerance" as the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

- developing strong reporting systems and analysis that incorporate quantitative and qualitative information to provide effective portfolio views of risk;

- identifying emerging risks, concentrations of risk, and other situations that could be properly assessed; and

- elevating critical issues to appropriate levels within an agency in a timely fashion.

To support this process and oversee the establishment of the agency's risk profile, regular assessment of risk, and development of appropriate risk response, an agency's governance structure may include a Risk Management Council or similar body. In addition, an agency may designate a Chief Risk Officer to help business unit managers integrate ERM practices into the agency's day-to-day business operations and decision-making. This may allow managers to identify issues in a timely manner and can facilitate data-driven decision-making.

Risk Profiles. Each agency must maintain and, at least annually, update a risk profile to (1) provide an analysis of the risks the agency faces in achieving strategic objectives arising from activities and operations, (2) identify appropriate options for addressing significant risks, and (3) inform the development of strategic plans as well as the President's budget. While agencies are required to maintain risk profiles, they were not subject to OMB review in fiscal years (FY) 2017 through 2019. Agencies have discretion in terms of the appropriate content and format for their risk profile; however, in general, risk profiles should include the following seven components:

1. *Identification of Objectives* – Specific strategic, operations, reporting, and compliance objectives must be identified and documented to facilitate identifying risks in these areas.

2. *Identification of Risk* – Risks should be initially identified by using a structured and systematic approach to recognize where the potential for undesired outcomes or opportunities can arise. Once initial risks are identified, it is important to re-examine risks on a regular basis to identify new risks or changes to existing risks.

3. *Inherent Risk Assessment* – OMB Circular No. A-123 defines "inherent risk" as the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations. Inherent risks should be ranked by appropriate categories, based on the impact and likelihood that each risk might occur.

4. *Current Risk Response* – Risk response (that is, the action taken to manage the risk) may involve risk acceptance, avoidance, reduction, or sharing. Formulation of risk responses should consider the agency's risk appetite and tolerance levels.

5. *Residual Risk Assessment* – The residual risk assessment involves identifying the exposure remaining from an inherent risk after action has been taken to manage it, and (using the same assessment standards as the inherent assessment) ranking the residual risk by category, based on the impact and likelihood that each risk might occur.

6. *Proposed Action* – Proposed actions are any additional actions taken to further reduce the exposure of residual risk.

7. *Proposed Risk Response Category* – Responsible officials should identify existing management processes to implement and monitor the proposed actions identified in step 6.

Implementation. At least annually, agencies should determine whether their risk profiles have changed, update risks as needed, and assess all aspects of the risk management process. In addition, agencies must integrate ERM processes with existing strategic reviews and internal control processes required by GPRAMA and FMFIA, as described below.

1. *Integrate with Strategic Reviews* – Key findings from agency risk profiles should be made available for discussion with OMB as part of the Agency Strategic Review meeting required by OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget.*

2. *Integrate with Management's Evaluation of Internal Control* – Beginning in FY 2017, agencies were expected to integrate ERM into management's evaluation of internal control reported in the Agency Financial Report or the Performance and Accountability Report. Generally, Agency Financial Reports and Performance and Accountability Reports are issued in November. Until an agency has fully implemented an ERM approach, agencies may provide existing risk assurance statements to their OIG and/or private accounting firms.

OMB circulars, including Circular No. A-123, are available for download at *https://www.whitehouse.gov/omb/information-for-agencies/circulars/*.

COSO ERM Integrated Framework

In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Board commissioned and published the ERM Integrated Framework, which is one of the most widely recognized and applied risk management frameworks. Over the past decade, the publication has gained broad acceptance by organizations in their efforts to manage risk. However, since 2004, the complexity of risk has changed, new risks have emerged, and both boards and executives have enhanced their awareness and oversight of ERM while asking for improved risk reporting. The COSO Board updated the framework in 2017 to address the evolution of ERM and the need for organizations to improve their approaches to managing risk to meet the demands of an evolving business environment. The updated document, *Enterprise Risk Management—Integrating with Strategy and Performance* (June 2017), highlights the importance of considering risk in both the strategy-setting process and in driving performance. More information is available at *www.coso.org*.

GAO Green Book

As previously discussed, good systems of internal control covering all aspects of an entity's objectives (operations, reporting, and compliance) are an integral part of ERM. FMFIA requires that Federal agency executives periodically review and annually report on the agency's internal control systems. FMFIA also requires the Comptroller General to prescribe internal controls standards. First issued in 1983, GAO's Green Book presents the internal control standards for Federal agencies to follow for both program and financial management, and the overall framework for establishing and maintaining an effective internal control system. The most recent revision of the Green Book, published in 2014, aligns the 17 COSO principles to the components of the existing internal control framework and adapts the principles to the federal government environment. The Green Book is available for download at *www.gao.gov*.

GAO Framework for Managing Fraud Risks in Federal Programs

Fraud poses a significant risk to the integrity of Federal programs and erodes public trust in government. Managers of Federal programs maintain the primary responsibility for enhancing program integrity. Legislation, guidance by the OMB, and new internal control standards have increasingly focused on the need for program managers to take a strategic approach to managing improper payments and risks, including fraud. GAO's framework for managing fraud risks in Federal programs (Framework)[14] identifies leading practices and conceptualizes the practices to assist in managing fraud risks. The Framework encompasses control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks. In addition, the Framework highlights the importance of monitoring and incorporating feedback. According to OMB Circular No. A-123, managers should adhere to these leading practices as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. Managers are responsible for determining the extent to which the leading practices in the Framework are relevant to their program and for tailoring the practices, as appropriate, to align with the program's operations. The Framework is available for download at *www.gao.gov*.

ERM Playbook

The ERM Playbook (Playbook)[15] is the result of an interagency effort to gather, define, and illustrate practices in applying ERM in the Federal context. The Playbook and accompanying appendices are tools designed to help Government departments and agencies meet the requirements of OMB Circular No. A-123, and to promote a common understanding of ERM practices. Nothing in the Playbook should be considered prescriptive and all examples provided should be modified to fit the circumstances, conditions, and structure of each agency (or other

[14] U.S. Government Accountability Office, *A Framework for Managing Fraud Risks in Federal Programs* (GAO-15-593SP; July 2015).

[15] The Chief Financial Officers Council and the Performance Improvement Council, *Playbook: Enterprise Risk Management for the U.S. Federal Government*; July 29, 2016.

Government organization). The Playbook, which can be downloaded at *www.cfo.gov*, is intended as a useful tool for management and not a standard for audit or other compliance reviews.

To help agencies establish comprehensive and effective ERM programs, the Playbook identifies the following six "ERM pitfalls":

1. **Focusing Too Much on Internal Controls.** ERM includes internal controls but also larger issues of the external environment, as well as transparency, business practices, reporting, and governance that help define the overall risk culture.

2. **Too Much Too Quickly.** ERM is an iterative effort that develops over time. Management may consider an incremental approach, initially focusing on the top two or three risks or a type of risk. Success in a specific area can illustrate the benefits of ERM and build the foundation for future efforts. Trying to change the fabric of an agency too much or too quickly could result in defensive mechanisms within the agency hampering ERM efforts.

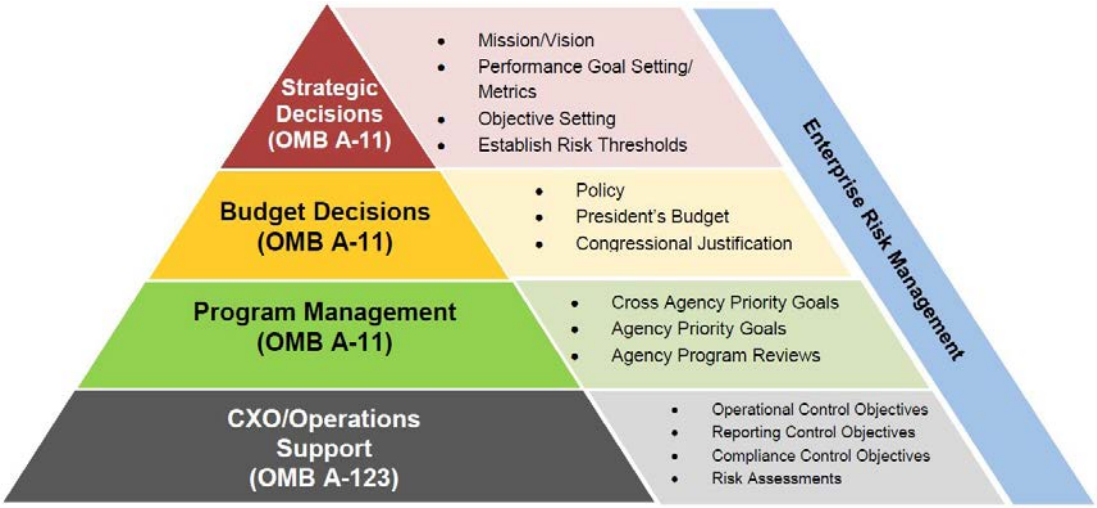
3. **Absence of Support from Senior Leaders.** Strong leadership at the top of the organization, including active participation in oversight, is extremely important for achieving success in an ERM program. ERM also requires active involvement and commitment from leaders in each business and program area (i.e., across silos) to develop and maintain a risk aware culture.

4. **Lack of a Core Team.** Each agency should assess the level of support necessary to implement and manage ERM effectively. To be effective, the ERM program will need the appropriate team with knowledge and experience in risk management, leadership, and gravitas to build the ERM function. While agencies should be careful about building an ERM empire, the size of the ERM team should reflect the needs of the organization to support effective risk management.

5. **Failure to Work Closely With Program Leaders.** In building out an ERM program, it is best to work with those within the agency that already own and manage risk to gain insights into the most significant and relevant risks facing the organization. It is an ERM program's role and responsibility to provide risk management assistance to others in the agency, not the other way around.

6. **ERM Not Integrated.** ERM should not be an isolated exercise, but instead, should be integrated into the management of the organization and eventually into its culture. ERM processes established in OMB Circular No. A-123 complement OMB Circular No. A-11, which discusses agency responsibilities for identifying and managing strategic and programmatic risk as part of agency strategic planning, performance management, and performance reporting practices. Together, these two Circulars constitute the core of the ERM policy framework for the Federal Government with specific ERM activities integrated and operationalized by Federal agencies. Figure 2 shows the interplay among OMB Circulars No. A-123 and A-11 and controls, program management, budget, and strategic decisions within the ERM framework.

Figure 2. The ERM Policy Framework



Source: The ERM Playbook.

To help OIGs assess the effectiveness of agency ERM programs, Exhibit A of this document provides possible audit or evaluation steps that incorporate the six common pitfalls discussed in the ERM Playbook.

ISO 31000:2018, Risk Management – Guidelines

International Organization for Standardization (ISO) 31000:2018 provides principles, a framework, and a process for managing risk, and can be used by any organization regardless of its size, activity, or sector. According to ISO, "Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment." The document also provides guidance for internal or external audit programs. Agencies using it can compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management and corporate governance. More information on ISO 31000:2018 is available at *www.iso.org*.

IIA Practice Guide

In December 2010, the Institute of Internal Auditors (IIA) released a practice guide intended to assist internal auditors with measuring the effectiveness of an organization's risk management and forming conclusions about the organization's level of risk management maturity. The IIA Practice Guide (Practice Guide)[16] uses the 2010 version of ISO 31000 as a basis for the risk

[16] The Institute of Internal Auditors, *IPPF-Practice Guide: Assessing the Adequacy of Risk Management Using ISO 31000*, December 2010.

management framework, although it acknowledges that other frameworks may be used.[17] The Practice Guide is available for download by IIA members at *www.theiia.org*.

According to the Practice Guide, different approaches to assessing an organization's risk management approach offer different perspectives on the effectiveness of the organization's process. The Practice Guide states, "The risk management process should be appropriately tailored to the organization, its size, culture, objectives, and risk profile. Therefore, the assurance process also needs to be tailored to the organization's needs." The Practice Guide further states that auditors can use any of the following three approaches, which are further discussed below:

1. Process Elements Approach
2. Key Principles Approach
3. Maturity Model Approach

Process Elements Approach. This approach checks whether each of the following seven ISO 31000-recognized elements of the risk management process is in place.

1. Communication: Sound risk management requires structured and ongoing communication and consulting with those who are affected by the operations of the organization or activity.
2. Setting the Context: The external environment (political, social, etc.) and internal environment (objectives, strategies, structures, ethics, discipline, etc.) of the organization or activity must be understood before the full range of risks can be identified.
3. Risk Identification: Identifying the risks should be a formal, structured process that considers sources of risk, areas of impact, and potential events and their causes and consequences.
4. Risk Analysis: The organization should use a formal technique to consider the consequence and likelihood of each risk.
5. Risk Evaluation: The organization should have a mechanism to rank the relative importance of each risk so that a treatment priority can be established.
6. Risk Treatment: Sound risk management requires rational decisions about risk treatment. Classically, such treatment is to avoid the activity from which the risk arises, share the risk, manage the risk by the application of controls, or accept the risk and take no further action.
7. Monitor and Review: Monitoring includes checking the progress of treatment plans, monitoring controls and their effectiveness, ensuring that proscribed activities are

[17] As previously stated, ISO updated ISO 31000 in 2018.

avoided, and checking that the environment has not changed in a way that affects the risks.

Key Principles Approach. Using this approach, auditors assess to what extent the organization's risk management process meets a minimum set of ISO 31000-recognized principles, which should ensure that risk management:

- creates and protects value;
- is an integral part of organization processes;
- is part of decision-making;
- explicitly addresses uncertainty;
- is systematic, structured, and timely;
- is based on the best available information;
- is tailored to match the operations of the organization;
- considers human and cultural factors;
- is transparent and inclusive;
- is dynamic, iterative, and responsive to change; and
- facilitates continual improvement and enhancement of the organization.

Maturity Model Approach. The maturity model approach builds on the assertion that the quality of an organization's risk management process should improve with time. A key aspect of this approach is the linking of risk management performance and progress in the execution of a risk management plan to a performance measurement and management system. The components for such a system normally consist of:

- A protocol of performance standards, considering current approaches to risk management and anticipating future strategic needs. Performance standards are normally supported by a list of more detailed performance requirements that enable measurement of any improvement in performance.
- A guide to how the standards and sub-requirements can be satisfied in practice.
- A means of measuring actual performance against each standard and sub-requirement.
- A means of recording and reporting performance and improvements in performance.
- The periodic independent verification of management's assessment.

In January 2017, the IIA also published an implementation guide for risk management, which provides recommended guidance for internal auditors on evaluating the effectiveness and contributing to the improvement of risk management processes.[18] In March 2019, the IIA released supplemental guidance on assessing the risk management process, which provides examples of risk management maturity models and a basic methodology internal auditors may use to provide independent assurance that the organization's risk management process is effective.[19]

[18] The Institute of Internal Auditors, *IPPF Implementation Guide 2120: Standard 2120 – Risk Management*, January 2017.

[19] The Institute of Internal Auditors, *IPPF Supplemental Guidance Practice Guide: Assessing the Risk Management Process*, March 2019.

PRIOR REVIEWS

As Federal ERM requirements and guidance have evolved, OIGs and GAO have sought to assess agency ERM programs and practices. To help OIGs meet professional standards related to audit and evaluation planning, below are high-level summaries of various ERM reviews completed in 2016 and 2018. Other relevant prior work may exist. OIGs should consult *www.oversight.gov* and *www.gao.gov*, among other sources of information, to identify additional reviews as they are completed. Each of the reports summarized below is available on the relevant OIG's website.

OIG

2016

- On July 12, 2016, the Treasury Inspector General for Tax Administration (TIGTA) issued a report on its audit of the IRS's efforts to implement a comprehensive process for identifying and mitigating significant risks to effective tax administration.[20] Among other things, TIGTA reported that the IRS had made significant progress in its efforts to implement an ERM program to provide a structured framework for the identification and mitigation of significant organizational risks.

- On October 28, 2016, the National Archives and Records Administration OIG (NARA OIG) issued an independent public accounting firm's report on its enterprise-wide risk assessment of NARA's internal controls and the risks to NARA's operations and procedures.[21] Among other things, the report noted that, while NARA appeared to be aware of significant risks and challenges, NARA had yet to implement an ERM program that clearly identified, prioritized, and managed risks throughout the organization.

- On December 2, 2016, the Export-Import Bank of the United States OIG (EXIM OIG) issued a report on its evaluation of risk management procedures and Chief Risk Officer responsibilities.[22] Among other things, EXIM OIG reported benchmarking EXIM Bank's key risk management policies with OMB and GAO guidance on ERM and internal controls, as well as current ERM practices as observed by a select group of peers, and identifying further actions needed to develop the Bank's integrated risk management program.

[20] Treasury Inspector General for Tax Administration, *Significant Progress Has Been Made in Implementing an Enterprise Risk Management Program* (2016-10-051; July 12, 2016).

[21] Cotton & Company LLP, *Enterprise-Wide Risk Assessment Audit of NARA's Internal Controls* (National Archives and Records Administration, Office of Inspector General Report No. 17-AUD-01; October 28, 2016).

[22] Export Import Bank of the United States, Office of Inspector General, *Evaluation of Risk Management Procedures and Chief Risk Officer Responsibilities* (Report No. OIG-EV-17-01; December 2, 2016).

2018

- On July 9, 2018, the U.S. Railroad Retirement Board OIG (RRB OIG) issued a report on its audit of the ERM process at the U.S. Railroad Retirement Board (RRB).[23] Among other things, RRB OIG reported that the RRB's ERM process was not fully effective. Specifically, RRB had not complied with all of the internal control requirements in OMB Circular No. A-123, did not implement the ERM process agencywide, and had not timely implemented prior audit recommendations.

- On July 16, 2018, the Library of Congress OIG (LOC OIG) issued a report on its evaluation of the Library of Congress's (Library) strategic planning and performance management efforts.[24] The objective of the evaluation was to analyze the steps taken to develop a more robust Library-wide strategic plan supported by aligned service unit plans and an integrated ERM framework. Among other things, LOC OIG reported that, although the Library did not have a fully mature ERM, the Library had developed, piloted, and launched a new Library-wide risk and internal controls approach that (a) aligned with annual performance goals and key business processes; (b) included the identification and assessment of risks and the development of responses to the risks; (c) incorporated the monitoring of risks and risk responses on an ongoing basis; and (d) involved ongoing reporting of risks, risk responses, and corrective actions.

- On July 24, 2018, the U.S. Department of Education OIG (ED OIG) issued a report on the extent to which the U.S. Department of Education's Office of Federal Student Aid implemented its ERM framework.[25] Among other things, ED OIG reported that the Office of Federal Student Aid developed an ERM framework, established a risk management office, and created a risk management committee; however, the organization did not implement all elements of its ERM framework or implement all elements characteristic of effective ERM.

GAO

In a December 2016 report, GAO sought to (1) update its risk management framework to more fully include evolving requirements and essential ERM elements, and (2) identify good practices that selected agencies have taken that illustrate those essential elements.[26] GAO reviewed literature to identify good ERM practices that generally aligned with the essential elements and validated these with subject matter specialists. GAO also met with officials from the 24 Chief Financial Officer Act agencies to discuss ERM activities and reviewed documentation where

[23] U.S. Railroad Retirement Board, Office of Inspector General, *Enterprise Risk Management Process at the Railroad Retirement Board Was Not Fully Effective* (Report No. 18-07; July 9, 2018).

[24] Library of Congress, Office of Inspector General, *Continued, Persistent Focus Needed to Strengthen the Library's Strategic Planning and Performance Management* (Report No. 2018-SP-103; July 16, 2018).

[25] U.S. Department of Education, Office of Inspector General, *Federal Student Aid: Efforts to Implement Enterprise Risk Management Have Not Included All Elements of Effective Risk Management* (ED-OIG/A05Q0007; July 24, 2018).

[26] U.S. Government Accountability Office, *Selected Agencies' Experiences Illustrate Good Practices in Managing Risk* (GAO-17-63; December 1, 2016).

available to corroborate officials' statements. According to GAO's report, a number of different frameworks exist for ERM. However, as shown in Figure 3, GAO outlined the following six essential elements for an agency to carry out ERM effectively:

1. aligning the ERM process to goals and objectives,
2. identifying risks,
3. assessing risks,
4. selecting risk responses,
5. monitoring risks, and
6. communicating and reporting on risks.

Figure 3 also provides the good practices that GAO reported agencies are implementing across the Federal Government.

Figure 3. GAO Table of Essential Elements and Associated Good Practices of Federal Government ERM Programs

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-17-63

In its report, GAO explained that the six essential elements fit together to form a continuing process for managing enterprise risks and the absence of any one element would likely result in an agency incompletely identifying and managing enterprise risk. For example, GAO stated that if an agency did not monitor risks, then it would have no way to ensure that it had responded to risks successfully. Although GAO recognized that that there is no "one right" ERM framework that all organizations should adopt, it reported that agencies should include the six essential elements in their ERM program.

EXHIBIT A: POSSIBLE STEPS TO CONSIDER WHEN ASSESSING AGENCY ERM PROGRAMS

The following are steps OIGs may consider when assessing agency ERM programs. These steps take into consideration the essential elements of ERM, the good practices that GAO identified in its December 2016 report, and the common pitfalls identified by the ERM Playbook. However, the specific steps auditors and evaluators perform will depend on the objectives and scope of their engagements, among other things.

General Information Related to the Agency's ERM Program

1. Identify the agency's values, beliefs, and attitudes toward ERM.
2. Determine whether the ERM program has engagement from management (including resources in relation to risks) and is appropriately situated within the agency, ensuring the responsible senior leader(s) is/are accountable for enterprise risks associated with the agency's strategic goals and objectives.
3. Obtain and document a walkthrough of the agency's ERM program, including the ERM framework, the components of that framework, the communications process, the criteria used to develop the framework, and any relevant policies, processes, and procedures.
4. Identify any prior internal or external audits, evaluations, or other reviews related to the agency's ERM program.
5. Gain an understanding of the agency's risk appetite (the amount of risk the agency is willing to accept in pursuit of its mission and vision). (NOTE: Risk appetite may differ in different areas of the agency's operations.)
6. Identify who within the agency (i.e management, program leaders, etc.) was involved in developing the ERM program, including the ERM framework and risk appetite, and what guidance was used. Determine whether the risk appetite was considered at the proper level in the governance structure.
7. Determine whether the agency used outside consultants for any aspect of ERM development, implementation, or ongoing management. If so, identify the consultants, the nature of their work, and any deliverables.
8. Identify those aspects of the agency's ERM program that the agency believes have been implemented and what, if any, the agency believes remains to be implemented.
9. Identify the core team and/or business units responsible for the agency's ERM program and other ERM-related roles and responsibilities.
10. Assess the ERM knowledge and skills of individuals responsible for risk analysis, evaluation, and treatment/response. Identify relevant ERM training that personnel have completed to determine whether individuals have been trained.

Objective Setting

11. Gain an understanding of the agency's processes for setting objectives and for ensuring objectives support the agency's mission.
12. Determine whether the agency's ERM program is aligned with strategic goals and objectives.
13. Determine whether the agency's ERM processes are integrated with strategic planning and organizational performance measurement processes and support budgeting, operational, and resource allocation activities.

Risk Identification

14. Determine the agency's process for identifying risks or opportunities at the business unit level that could positively or negatively affect business units' ability to achieve their objectives. Determine whether such information is used to identify potential enterprise-level risks.
15. Determine the agency's process for identifying risks or opportunities at an enterprise level that could positively or negatively affect the agency's ability to achieve its objectives. Identify the sources of information the agency uses to develop its list of risks.
16. Identify those risks or opportunities the agency found that could negatively or positively affect its ability to achieve its objectives.
17. Determine whether the agency has developed an organizational culture to encourage employees to identify and discuss risks openly.
18. Identify how the agency determines the likelihood of the risks or opportunities and the possible effect or impact.

Risk Assessment

19. Evaluate the agency's process for assessing risks or opportunities that affect its ability to achieve its objectives.
20. Identify the process by which risks are analyzed in relation to the agency's strategic objectives. Determine whether the agency modifies its strategic objectives based on the results of risk assessments.

Risk Response and Control Activities

21. Determine the action(s) the agency takes after identifying enterprise-level risks.
22. Determine the context and other potential barriers, (resources, culture, legislation, programmatic design, etc.) that may hamper management's risk response.
23. Assess the agency's processes for ensuring actions and risk responses are effectively carried out.

Information and Communication

24. Determine how the risks or opportunities identified within a business unit are communicated to the business unit manager and, as appropriate, other business units. If

those risks or opportunities rise to the enterprise-level, determine how they are communicated to the appropriate officials including agency leadership. Identify the actions, if any, taken to address the risks and opportunities by the appropriate officials.

25. Determine how general risk information (defined broadly) is communicated throughout the entity, both from the top down and bottom up. Risk information could be, qualitative, quantitative in nature, formal or informal.
26. Identify any external groups (general public, vendors, Congress, other external stakeholders, etc.) that receive information related to the agency's ERM program and determine whether external communication and reporting mechanisms comply with relevant legal, regulatory, corporate governance, and disclosure requirements. Identify specific information the agency provides, how the information is provided, and how often.
27. Determine whether communication with agency stakeholders adequately reflects the agency's attitude toward and treatment of risks.

Monitoring

28. Determine whether the agency monitors its ERM program. At a minimum, identify who conducts the monitoring, how often monitoring is performed, what reports or other output is produced from the monitoring and where the information gets reported, and whether performance measures exist.
29. Assess the process used to identify and implement corrective action(s) to address deficiencies identified through monitoring.
30. Assess the agency's process for improving the risk framework and related processes and controls as business conditions and organizational needs change.

EXHIBIT B: TRAINING RESOURCES

Through independent and objective audits and evaluations, OIGs can help Federal agencies' ERM programs succeed. However, OIG personnel must be knowledgeable of ERM requirements and principles before undertaking such engagements. OIGs' training needs may differ depending on, among other things, their agency's ERM program maturity, the OIG's knowledge of ERM, and the scope and objectives of planned engagements. The following table provides various ERM-related training opportunities that were available as of January 2020.[27] The table is organized by overall training topic and, for each course listed, provides the title, vendor, training format, course description, cost, and a link for more information.

Table. ERM Training Resources Available as of January 2020

TRAINING TOPIC: Developing and Integrating an ERM Program Within an Agency	
Course Title:	**ERM: A Driver for Organizational Success**
Vendor:	Institute of Internal Auditors
Format:	eLearning (Group-Internet-Based); On-site Training (Group-Live); Seminar (Group-Live)
Training Objective/ Description:	This course unpacks the theory behind ERM with group activities and real-world scenarios. This course is designed for internal auditors with at least 3 years of experience who are involved in the ERM process, as well as managers and other professionals who deal with the complexities of ERM. (16 CPEs)
Cost:	On-site: $1,295 for members; $1,565 for non-members eLearning: $1,195 for members; $1,465 for non-members
Course Information:	*https://na.theiia.org/training/courses/Pages/Enterprise-Risk-Management-A-Driver-for-Organizational-Success.aspx*
Course Title:	**ERM: Executive Seminar**
Vendor:	Graduate School USA
Format:	Classroom – Live
Training Objective/ Description:	This seminar is designed for managers, auditors, analysts, and executives responsible for mission and mission support risk assessment over financial and performance activities including implementing the Federal Manager's Financial Integrity Act and OMB Circular A-123. It is also designed for auditors and evaluators who need to understand the application and role of risk management and assessing internal control in sustaining organizational performance, efficiency, effectiveness, and accountability. (8 CPEs)
Cost:	$449
Course Information:	*http://register.graduateschool.edu/modules/shop/index.html?action=section&OfferingID=743*
Course Title:	**Develop and Execute an ERM System**
Vendor:	ComplianceOnline
Format:	Online/Webinar – Six Part Course Series

[27] Information on training resources is subject to change. OIGs should consult the websites provided for each course to obtain the most up-to-date information.

Table. ERM Training Resources Available as of January 2020

Training Objective/ Description:	The objective of this six part series of webinars is to arm internal auditors and risk managers with practical insights to enhance their skills to embed an effective enterprise-wide risk management process.
Cost:	$835 for unlimited viewing for one account for 6 months; $735 for one CD/USB, single location use
Course Information:	*https://www.complianceonline.com/develop-and-execute-an-enterprise-risk-management-erm-system-course-package-webinar-training-701725-prdw*
TRAINING TOPIC: Auditing ERM Programs	
Course Title:	**Internal Audit's Role in ERM**
Vendor:	ComplianceOnline
Format:	Online/Webinar
Training Objective/ Description:	This training on internal audit compliance will help the attendees understand the role and importance of audits in an ERM program. Learn assurance models and standards and how audit can help.
Cost:	$149 for unlimited viewing for one account for 6 months; $299 for one CD/USB, single location use
Course Information:	*https://www.complianceonline.com/internal-audits-role-in-enterprise-risk-management-webinar-training-703104-prdw*
Course Title:	**How to Audit the ERM Function**
Vendor:	ComplianceOnline
Format:	Online/Webinar
Training Objective/ Description:	This training will provide the attendees best practices for auditing the ERM function. Learn the role and importance of audit in maintaining the effectiveness of the ERM program.
Cost:	$149 for unlimited viewing for one account for 6 months; $199 for one CD/USB, single location use
Course Information:	*https://www.complianceonline.com/how-to-audit-the-erm-function-webinar-training-703240-prdw*
TRAINING TOPIC: General Knowledge of ERM and Risk Management	
Course Title:	**ERM Presentations and Training**
Vendor:	Association of Government Accountants
Format:	Webinars and PowerPoint Presentations
Training Objective/ Description:	The Association of Government Accountants maintains a Web page of various online training resources related to ERM. Topics include: "Enterprise Risk Management at the Architect of the Capitol," "Enterprise Risk Management: Stories from the Front Lines," and "Watchdog or Partner: Agencies and IGs in ERM/FRM Implementation."
Cost:	Free
Course Information:	*https://www.agacgfm.org/Tools-Resources/intergov/ERM-hub-home/ERM-Articles-and-Presentations.aspx*
Course Title:	**Association for Federal ERM (AFERM)**
Vendor:	AFERM

Table. ERM Training Resources Available as of January 2020

Format:	Annual Summit/Live Conference – Multi-Day (CPE Eligible); Also available are workshops, presentations, podcasts, and other ERM tools and resources
Training Objective/ Description:	The AFERM ERM summit is held once a year. The theme of the 2019 summit was "Next Generation of ERM: What You Need To Know." *Check the AFERM website for announcements of annual training dates/locations.
Cost:	AFERM Membership: $40 annually for government employees AFERM ERM Summit: $525 for Federal AFERM members and $625 for Federal employee non-members; $100 early bird discount available for both registrations
Course Information:	*https://www.aferm.org/events/2019-aferm-summit/*
TRAINING TOPIC: ERM Certificate Program	
Course Title:	**COSO ERM Certificate Program Online**
Vendor:	Institute of Internal Auditors
Format:	Online Self Study – On Demand
Training Objective/ Description:	The new COSO ERM Certificate offers participants the unique opportunity to learn the concepts and principles of the newly updated ERM framework and prepares participants to integrate the framework into individual organization's strategy-setting process to drive business performance. Participants should have exposure working with ERM (preferably at least 2-6 years' experience) and a basic level of exposure to COSO *ERM – Integrating with Strategy and Performance* (the ERM framework). (13.5 CPEs)
Cost:	$749 members only pricing; $939 for non-members
Course Information:	*https://ondemand.theiia.org/learn*
Course Title:	**COSO ERM Certificate Program**
Vendor:	Institute of Internal Auditors
Format:	eLearning (Group-Internet-Based); On-site Training (Group-Live); Seminar (Group-Live) – 2.5 days
Training Objective/ Description:	The new COSO ERM Certificate Program offers participants the unique opportunity to learn the concepts and principles of the updated ERM framework and to prepare participants to integrate the framework into individual organization's strategy-setting process to drive business performance. Participants should have exposure working with ERM (preferably at least 2-6 years' experience) and a basic level of exposure to COSO *ERM – Integrating with Strategy and Performance* (the ERM framework). (23 CPEs)
Cost:	$1,799 for members; $2,299 for non-members
Course Information:	*https://na.theiia.org/training/courses/Pages/COSO-Enterprise-Risk-Management-Certificate-Program.aspx#*