

# TAB B

## RISK ASSUMED II

### APPENDICES

Appendix A	Risk Assumed – Phase II: Project History and Milestones
Appendix B	OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (A-123)
Appendix C	OMB Circular No. A-11, Section 230, Agency Strategic Planning (A-11)
Appendix D	Federal Highway Administration Risk Management Process User Manual, 2013

FEBRUARY 2018

THIS PAGE INTENTIONALLY LEFT BLANK

TAB B

RISK ASSUMED II

APPENDIX A

Risk Assumed – Phase II:  
Project History and Milestones

FEBRUARY 2018

## PROJECT OBJECTIONS

The issuance of [Statement of Federal Financial Accounting Standards \(SFFAS\) 51, Insurance Programs](#), on January 18, 2017, effectively concluded the first phase of risk assumed. For the history of the risk assumed project and milestones for phase I, please see <http://www.fasab.gov/ra-insurance-programs/>.

In phase II, the Board will holistically review significant risk events other than adverse events covered by SFFAS 51, Insurance Programs, to determine accounting standards that provide concise, meaningful, and transparent information regarding the potential impact to the fiscal health of the federal government.

## HISTORY OF BOARD DELIBERATIONS

### October 19-20, 2016 Board Meeting

At the October 19, 2016, Board meeting, the risk assumed – phase II began.

The Board reviewed staff's high-level gap analysis presented in table 1: Analysis of Federal Accounting Standards in Relation to the IMF [International Monetary Fund] Recommendations for Disclosing Fiscal Risks and table 2 from the Australian Statement 8: Statement of Risks.

The Board agreed that an extensive gap analysis is necessary to determine the risk information that the consolidated financial report of the U.S. Government includes and how it is presented, the extent to which FASAB can align with enterprise risk management (ERM) as prescribed by The Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, and the Board's preference for presenting risk assumed information going forward.

For the gap analysis, the Board agreed to determine the following:

- If federal government reporting is transparent enough for estimates and uncertainty around significant risks with a focus on broad risk categories, such as an economic downturn where revenues go down and benefit program costs go up
- If there is a significant gap in reporting to be addressed for individual risk items, such as treaties, commitments by the federal government, and intergovernmental dependencies with state and local governments
- How to present summarized risk events at the government-wide level for cross-cutting agency efforts, such as disaster relief, with access to detail at the agency level

**December 19-20, 2016**

At the December 20, 2016, Board meeting, the Board approved a framework for the risk assumed gap analysis. Members agreed that categories should not be a laundry list of events but instead should be principle-based and broad enough to encompass current and future significant risk events. The scope will include past and future events and whether uncertainty is adequately explained. Staff will review past financial reports to understand what was included before and after recent large events, such as the 2008 financial crisis, at the agency and government-wide levels.

Staff will utilize roundtable discussions to discover if current disclosures are clear, relevant, and add value in relation to the available standards. If roundtable participants do not feel that current disclosures are clear, relevant, or valuable, the group will discuss what is missing and should be included.

Staff will work on the gap analysis over the next several months and present findings and recommendations to the Board upon completion.

**June 21-22, 2017**

Members did **not** want to include discussions that

- predict unforeseen catastrophes and their potential financial effect;
- trends for using emergency funding as an indicator of fiscal exposure to risk shocks;
- comparisons of estimates to actuals;
- how past risk events were managed; or
- a separate risk section [as presented in the USAFacts 10-K Report -risk section—Item 1A Risk Factors] within federal financial reports.

Members **did want to**

- include past events that affect the current financial position;
- include and define major risk events with a relationship to long-term sustainability that are not already reported;
- use the principle-based broad risk categories as a foundation for continuing the gap analysis; and
- present meaningful streamlined information as a broad analysis rather than specific details.

**October 25-26, 2017**

According to the project objective, the risk assumed project strives ... to determine accounting standards that provide concise, meaningful, and transparent information regarding the potential impact to the fiscal health of the federal government. However, understanding what risks affect U.S. financial sustainability and why they do is very challenging. Therefore, as part of the ongoing gap analysis, staff reviewed SFFAS 2, Accounting for Direct Loans and Loan Guarantees, to learn how risk is currently disclosed in the financial statements.

Staff conducted research with the Department of Education, Department of Housing and Urban Development, Small Business Administration, and the Government Accountability Office and learned that agencies cannot specifically identify their users. In addition, reporting is inconsistent, extremely detailed, and burdensome. This not only affects preparers, but also users.

On October 26, 2017, staff presented these findings at the Board meeting to determine if members wanted to pilot amendments to SFFAS 2 to develop a framework for how to address risk assumed holistically.

Members agreed and requested that staff

- identify user groups to analyze risk factors, beyond those used to calculate credit subsidy reestimates, to help build a risk profile;
- develop a framework for how to discuss measurement uncertainty;
- consider how to discuss the “why” behind the “what” of risk;
- present sensitivity analysis at a future meeting; and
- pilot amendments to SFFAS 2 to develop a model/framework for how to address risk assumed holistically.

TAB B

RISK ASSUMED II

APPENDIX B

OMB Circular No. A-123, Management's  
Responsibility for Enterprise Risk  
Management and Internal Control (A-123)

FEBRUARY 2018



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

THE DIRECTOR

July 15, 2016

M-16-17

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan  
Director

SUBJECT: OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

The Administration has emphasized the importance of having appropriate risk management processes and systems to identify challenges early, to bring them to the attention of Agency leadership, and to develop solutions. To that end, the Office of Management and Budget (OMB) is updating this Circular to ensure Federal managers are effectively managing risks an Agency faces toward achieving its strategic objectives and arising from its activities and operations. These expanded responsibilities reinforce the purposes of the Federal Managers' Financial Integrity Act (FMFIA) and the Government Performance and Results Act Modernization Act (GPRAMA), and support the Administration's commitment to improve the efficiency and effectiveness of Government.

Since 1981, OMB Circular No. A-123 (A-123) and FMFIA have been at the center of Federal requirements to improve accountability in Federal programs and operations. Over the years, government operations have changed dramatically, becoming increasingly complex and driven by changes in technology. At the same time, resources are constrained and stakeholders expect greater program integrity, efficiency and transparency into government operations.

The policy changes in this Circular modernize existing efforts by requiring agencies to implement an Enterprise Risk Management (ERM) capability coordinated with the strategic planning and strategic review process established by GPRAMA, and the internal control processes required by FMFIA and Government Accountability Office (GAO)'s Green Book. This integrated governance structure will improve mission delivery, reduce costs, and focus corrective actions towards key risks. Implementation of this policy will engage all agency management, beyond the traditional ownership of OMB Circular No. A-123 by the Chief Financial Officer community. In particular, it will require leadership from the agency Chief Operating Officer and Performance Improvement Officer, and close collaboration across all agency mission and mission-support functions.



Successful implementation of this 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. Similarly, agency managers, Inspectors General (IG) and other auditors should establish a new set of parameters encouraging the free flow of information about agency risk points and corrective measure adoption. An open and transparent culture results in the earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a more resilient government.

This revision of the Circular has gone through an extensive deliberative process with Agencies and their IG teams, and including consultation with the GAO and many outside groups who seek more efficient and effective delivery of governmental services. This revised Circular is effective for Fiscal Year (FY) 2016 and supersedes all previous versions. Appendices A, B, C, and D of OMB Circular No. A-123 remain in effect. Updates to the GAO greenbook are effective for FY 2016. ERM implementation requirements are effective for FY 2017. OMB plans to work closely with the President's Management Council, Executive Councils, and the Council of Inspectors General on Integrity and Efficiency (CIGIE) to provide further implementation guidance.

Attachment:

OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

## ATTACHMENT

### OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

**Purpose:** This Circular defines management's responsibilities for enterprise risk management (ERM) and internal control. The Circular provides updated implementation guidance to Federal managers to improve accountability and effectiveness of Federal programs as well as mission-support operations through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness. The Circular emphasizes the need to integrate and coordinate risk management and strong and effective internal control into existing business activities and as an integral part of managing an Agency.

**Authority:** This Circular is issued under the authority of the Federal Managers' Financial Integrity Act (FMFIA) of 1982 as codified in 31 U.S.C. 3512, and the Government Performance Results Act (GPRA) Modernization Act, Public Law 111-352.

**Policy:** Each Federal employee is responsible for safeguarding Federal assets and the efficient delivery of services to the public. Federal leaders and managers are responsible for establishing goals and objectives around operating environments, ensuring compliance with relevant laws and regulations, and managing both expected and unexpected or unanticipated events. They are responsible for implementing management practices that identify, assess, respond, and report on risks. Risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats and to identify previously unknown opportunities to improve the efficiency and effectiveness of government operations. Management is also responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance. Management must consistently apply these internal control standards to meet the internal control principles and related components outlined in this circular and to assess and report on internal control effectiveness at least annually. Risk management practices must be taken into account when designing internal controls and assessing their effectiveness. Annually, agencies must develop a risk profile coordinated with their annual strategic reviews. Further, management must provide assurances on internal control effectiveness in its Agency Financial Report (AFR) or the Performance and Accountability Report (PAR). Information regarding identified material weaknesses and corrective actions should be included in any of the three preceding reports.

**Requirements:** Office of Management and Budget (OMB) Circular No. A-123 requires agencies to integrate risk management and internal control functions. The Circular also establishes an assessment process based on the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (known as the [Green Book](#)) that management must implement in order to properly assess and improve internal controls over operations, reporting, and compliance. The primary compliance indicators that management must consider when implementing OMB Circular No. A-123, include:

- Management is responsible for the establishment of a governance structure to effectively implement, direct and oversee implementation of the Circular and all the provisions of a robust process of risk management and internal control.
- Implementation of the Circular should leverage existing offices or functions within the organization that currently monitor risks and the effectiveness of the organization's internal control.
- Agencies should develop a maturity model approach<sup>1</sup> to the adoption of an ERM framework. For FY 2016, Agencies are encouraged to develop an approach to implement ERM. For FY 2017 and thereafter Agencies must continuously build risk identification capabilities into the framework to identify new or emerging risks, and/or changes in existing risks (See Section II.C. for additional details).
- Management must evaluate the effectiveness of internal controls annually using GAO's *Standards for Internal Control in the Federal Government*. (The [Green Book](#))

Throughout the Circular, the terms “Must” and “Will” denote a requirement that management will comply with in all cases. “Should,” indicates a presumptively mandatory requirement except in circumstances where the requirement is not relevant for the Agency. “May” or “Could,” indicate best practices that may be adopted at the discretion of management.

**Effective Date:** This Circular is effective upon publication. Appendices A, B, C, and D of OMB Circular No. A-123 remain in effect.

**Applicability:** This Circular is applicable to each executive agency. All other non-executive agencies of the Federal government are encouraged to adopt the Circular.

**Inquiries:** Further information concerning this Circular can be obtained from the Office of Federal Financial Management (202) 395-3993 or the Office of Performance and Personnel Management, (202) 395-5670 Office of Management and Budget, Washington, DC 20503.

**Copies:** Copies of this Circular may be obtained from [www.whitehouse.gov/omb](http://www.whitehouse.gov/omb).

---

<sup>1</sup> See <https://www.rims.org/resources/ERM/Pages/RiskMaturityModel.aspx> for an example maturity model.

## Significant Revisions to OMB Circular No. A-123

Section	Revision to A-123	Purpose of Revision
Transmittal to the Circular	Changed title from OMB Circular No. A-123, Management's Responsibility for Internal Control to OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control	Title changed to align better with the focus of the Circular towards an enterprise risk management framework.
Restructure	Former Section I, Introduction, Section II, Standards, and Section III, Integrated Internal Control Framework restructured as described below. <i>Appendix A, Internal Control Over Financial Reporting (ICOFR)</i> removed from the body of A-123 and renamed to <i>Appendix A, Internal Control Over Reporting (ICOR)</i>	Introduce Enterprise Risk Management guidance; eliminate areas of duplication; and balance emphasis on operations, compliance, and reporting.  Based on the significance of GAO <i>Standards for Internal Control</i> changes related to internal control over reporting; OMB plans to issue the prior Appendix A as a standalone document. Appendices A, B, C, and D of OMB Circular No. A-123 remain in effect.
Throughout Circular	Referenced ERM concepts and guidelines based on the Committee of Sponsoring Organizations of the Treadway Commission (COSO), International Organization for Standards (ISO) and the United Kingdom's Orange Book, <i>Management of Risk – Principles and Concepts</i> . <sup>2</sup>	Provide additional ERM implementation guidance.
Section I. Introduction	Changed the focus of the Introduction to illustrate management's responsibility to manage risk, the relationships between A-123 and Part 6 of A-11, <i>Federal Performance Framework, and Internal Controls and Enterprise Risk Management</i> .	Provide an overview of the integration of Internal Controls and Enterprise Risk Management
Section II. Establishing Enterprise Risk Management in Management Practices	Addition of a new section.	Provide for more effective risk management and internal control in the Federal Government.
Section III. Establishing and Operating an Effective Internal Control System	Addition of a new section.	Provide evaluation guidance for the new GAO <a href="#">Green Book</a> .

---

<sup>2</sup> References to non-Federal Government entities are provided to illustrate best practices and do not signify endorsement by the Federal Government.

Section	Revision to A-123	Purpose of Revision
Section IV. Assessing Internal Control	Included a summary of updated Standards of Internal Control in the Federal Government and related documentation and assessment requirements.	Provide evaluation guidance for the new GAO <a href="#">Green Book</a> .
Section V. Correcting Internal Control Deficiencies	Included minimum requirements for corrective action plans.	Emphasize root cause analysis, accountability, and collaboration with Offices of Inspectors General.
Section VI. Reporting on Internal Control	Requires a single assurance statement consistent with the original requirement of the Federal managers Financial Integrity Act (FMFIA).	Provide a risk based approach and balance emphasis between operations, reporting, and compliance internal control objectives.
Section VII. Additional Considerations	Addition of a new section.	Provide additional considerations for emerging issues including: managing privacy risks, integrating acquisition assessments with the new GAO <a href="#">Green Book</a> , managing grant risks and managing Antideficiency Act risks.

## TABLE OF CONTENTS

I.	Introduction.....	7
II.	Establishing Enterprise Risk Management In Management Practices .....	9
A.	Governance.....	12
B.	Risk Profiles .....	13
B1.	Identification of Objectives.....	16
B2.	Identification of Risk .....	16
B3.	Inherent Risk Assessment.....	17
B4.	Current Risk Response.....	18
B5.	Residual Risk Assessment .....	19
B6.	Proposed Action.....	19
B7.	Proposed Risk Response Category .....	19
C.	Implementation.....	19
D.	Role of Auditors in Enterprise Risk Management.....	21
III.	Establishing And Operating An Effective System Of Internal Control .....	22
A.	Governance.....	23
B.	Establish Entity Level Control .....	24
B1.	Service Organizations .....	24
B2.	Managing Fraud Risks in Federal Programs.....	26
IV.	Assessing Internal Control.....	29
A.	Documentation Requirements .....	29
B.	Sources of Information .....	29
C.	Identification of Deficiencies .....	30
D.	Internal Control Evaluation Approach.....	31
V.	Correcting Internal Control Deficiencies .....	35
A.	Importance of Correcting Internal Control Deficiencies .....	35
B.	Corrective Action Plan Requirements .....	35
C.	Audit Follow Up and Cooperative Audit Resolution and Oversight Initiatives .....	36
VI.	Reporting on Internal Controls .....	37
A.	Annual Assurance Statement.....	37
B.	Reporting Pursuant to Integration of Enterprise Risk Management and Internal Control.....	37
C.	Reporting Pursuant to OMB Circular No. A-123, Appendix A.....	37
D.	Reporting Pursuant to OMB Circular No. A-130, Appendix I .....	38
E.	Reporting Pursuant to Section 2—31 U.S.C. 3512(d) (2) .....	38
F.	Reporting Pursuant to Section 4—31 U.S.C. 3512(d) (2) (B).....	38
G.	Government Corporations .....	39
H.	Classified Matters.....	39

I. Agencies Obtaining Audit Opinions on Internal Control .....	43
VII. Additional Considerations .....	44
A. Managing Privacy Risks in Federal Programs.....	44
B. Conducting Acquisition Assessments under OMB Circular No. A-123.....	46
C. Managing Grants Risks in Federal Programs .....	47
D. Managing Antideficiency Act Risks.....	48

## **LIST OF TABLES**

Table 1 Illustrative Example of a Risk Profile .....	15
Table 2 Summary of Green Book Components and Principles of Internal Control .....	23
Table 3 Illustrative Internal Control Evaluation – Control Environment .....	33
Table 4 Principle and Component Evaluation .....	33
Table 5 Overall Assessment of a System of Internal Control .....	34
Table 6 Summary of OMB Circular No. A-123 Reporting Requirements .....	40
Table 7 Comparison of OMB Acquisition Framework and GAO Green Book .....	47

## **LIST OF FIGURES**

Figure 1 The Relationship Between Internal Controls and Enterprise Risk Management.....	8
Figure 2 Illustrative Example of an Enterprise Risk Management Model.....	11
Figure 3 ERM Development and Implementation Deadlines .....	20

## **LIST OF EXHIBITS**

Exhibit 1 Illustrative Unmodified Assurance Statement .....	42
Exhibit 2 Illustrative Modified Assurance Statement .....	42
Exhibit 3 Illustrative Statement of No Assurance .....	43

## I. INTRODUCTION

Federal leaders and managers are responsible for establishing and achieving goals and objectives, seizing opportunities to improve effectiveness and efficiency of operations, providing reliable reporting, and maintaining compliance with relevant laws and regulations. They are also responsible for implementing management practices that effectively identify, assess, respond, and report on risks. Risks arise from a variety of external and internal environments. Examples include economic, operational, and organizational change factors, all of which would negatively impact an Agency's ability to meet goals and objectives if not resolved.

Federal leaders and managers achieve these aims through a governance structure defined through a variety of sources, including laws enacted by the Congress and numerous Executive directives and Agency policies. Most relevant to this discussion, the Federal Government's core governance processes are defined by Office of Management and Budget (OMB) budget guidance, such as [OMB Circular No. A-11](#), which defines the processes by which the Executive Branch develops and executes Strategic Plans, compiles the President's Budget request, assembles Congressional Budget Justifications, conducts performance reviews, and issues Annual Performance Plans and Annual Performance Reports. OMB Circular No. A-123 provides guidance to Federal Managers on improving the accountability and effectiveness of Federal programs and operations by identifying and managing risks, establishing requirements to assess, correct, and report on the effectiveness of internal controls.

Enterprise Risk Management (ERM) and Internal Control are components of a governance framework. ERM as a discipline deals with identifying, assessing, and managing risks. Through adequate risk management, agencies can concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events. Internal control is a processes effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.

Leading international standards setters in the fields of risk management and internal control including both the Committee of Sponsoring Organizations of the Treadway Commission ([COSO](#)) and the International Organization for Standardization (ISO) incorporate internal control as part of the larger risk management process. ERM is viewed as a part of the overall governance process, and internal controls as an integral part of risk management and ERM. This relationship is depicted in the following [COSO-based](#) diagram in Figure 1.



*Figure 1 The Relationship Between Internal Controls and Enterprise Risk Management*



The remaining sections of this document is organized as follows:

**Section II** of OMB Circular No. A-123 defines management’s responsibilities for ERM, and includes requirements for identifying and managing risks. Most importantly, it encourages agencies to establish a Risk Management Council (RMC), develop “Risk Profiles” which identify risks arising from mission and mission-support operations, and consider those risks as part of the annual strategic review process. It complements Section 270 of 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 ERM policy framework for the Federal Government, with specific ERM activities integrated and operationalized by Federal agencies.

**Section III** of OMB Circular No. A-123 includes guidance for establishing internal controls for those risks identified by management as requiring a formal system of internal control to provide reasonable assurance that objectives are achieved. For this subset of risks identified by management, this Circular prescribes requirements conforming with the Standards of Internal Control in the Federal Government established by the Government Accountability Office (GAO), more commonly known as the [Green Book](#). This includes establishing and maintaining internal control to achieve specific objectives related to operations, reporting, and compliance; assessing and reporting effectiveness; and providing assurances on its Agency Financial Report (AFR), or the Performance and Accountability Report (PAR). Information regarding identified material weaknesses and corrective actions should be included in any of the three preceding reports.

**Section IV** of OMB Circular No. A-123 discusses management’s responsibility to continuously monitor, assess, and improve the effectiveness of internal controls. Also discussed are documentation requirements, possible sources of information for use in the assessment on internal controls, identification of deficiencies and the internal control evaluation approach.

**Section V** of OMB Circular No. A-123 provides guidance on correcting internal control deficiencies, corrective action plan requirements and audit follow up and resolution initiatives. An Agency's corrective action process provides the ability for management to develop a plan for addressing the risk associated with a control deficiency. An Agency's ability to correct control deficiencies is an indicator of the strength of its internal control environment.

**Section VI** of OMB Circular No. A-123 provides guidance on annual assurance statements and reporting requirements in accordance with 31 U.S.C. 3512, (that allows for a single assurance statement), Government Corporations and classified matters. This section also provides definitions for a control deficiency, significant deficiency, and a material weakness.

**Section VII** of OMB Circular No. A-123 discusses additional considerations such as managing privacy risks, conducting acquisition assessments, managing risk to grants and managing Antideficiency Act risks.

## **II. ESTABLISHING ENTERPRISE RISK MANAGEMENT IN MANAGEMENT PRACTICES**

There are several Enterprise Risk Management (ERM) models available to help organizations integrate risk management and internal control activities into a common framework. Section 270.24 of the Office of Management and Budget (OMB) Circular No. A-11 defines "risk" as the effect of uncertainty on objectives. Risk management is a series of coordinated activities to direct and control challenges or threats to achieving an organization's goals and objectives. ERM is an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery. While agencies cannot respond to all risks related to achieving strategic objectives and performance goals, they must identify, measure, and assess risks related to mission delivery. Effective risk management:

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

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

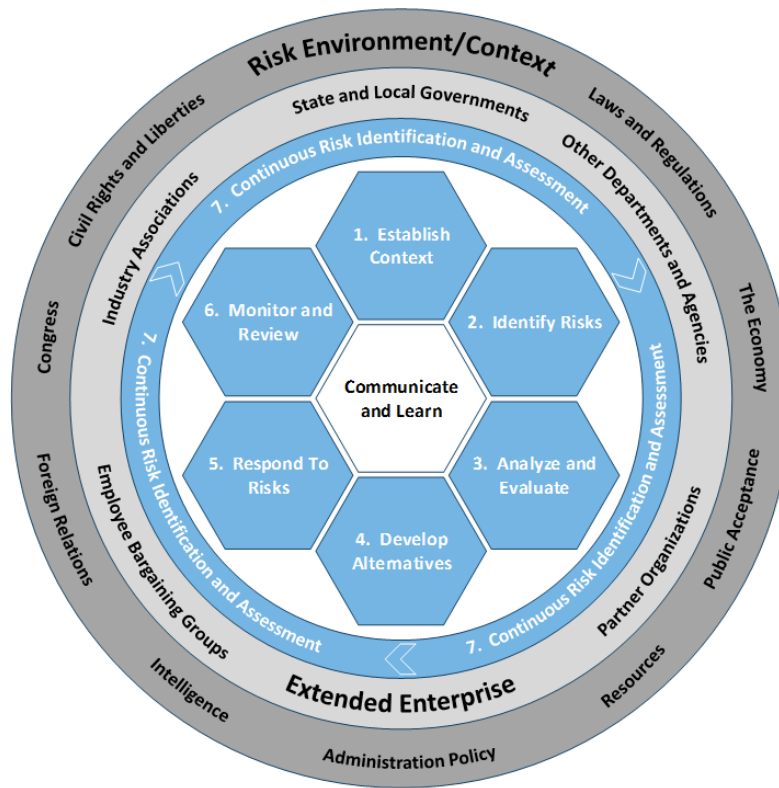
- ***Risk appetite-*** is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives.
- ***Risk tolerance-*** is the acceptable 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.
- ***A portfolio view of risk-*** provides insight into all areas of organizational exposure to risk (such as reputational, programmatic performance, financial, information technology, acquisitions, human capital, etc.), thus increasing an Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment.

ERM is beneficial since it addresses a fundamental organizational issue: the need for information about major risks to flow both up and down the organization and across its organizational structures to improve the quality of decision-making. ERM seeks to open channels of communication so that managers have access to the information they need to make sound decisions. ERM seeks to encompass the range of major risks that threatens agencies' ability to implement their missions, programs, and operations. Most agencies should build their capabilities, first to conduct more effective risk management, then to implement ERM, rating those risks in terms of impact, and finally building internal controls to monitor and assess the risk developments at various time points. To complete this circle of risk management the Agencies must incorporate risk awareness into the agencies' culture and ways of doing business. While there are many approaches that can be taken to implement ERM, most include the following elements:<sup>3</sup>

---

<sup>3</sup> Based on The Orange Book, Management of Risk – Principles and Concepts, October 2004, HM Treasury.

Figure 2 Illustrative Example of an Enterprise Risk Management Model



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

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

The risk environment is beyond the boundary of the “extended enterprise.” The environment generates risks that cannot be controlled, or constrain the way the organization is permitted to take on or address risk.

### **A. Governance**

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. Industry best practices suggest risk management functions generally have the following characteristics:

- helping senior management develop and implement core policies and procedures with respect to enterprise risk management, including developing a process to define risk appetite, and establish risk thresholds accordingly;
- ensuring the current risk levels and processes are consistent with the established risk tolerance thresholds and policies;
- supporting implementation of effective controls;
- 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 provide governance for the risk management function, agencies may use a Risk Management Council (RMC) to oversee the establishment of the Agency’s risk profile, regular assessment of risk, and development of appropriate risk response. RMC structures will vary by Agency, and in some cases may be integrated with existing management structures. An effective RMC will include senior officials for program operations and mission-support functions to help ensure those risks are identified which have the most significant impact on the mission outcomes of the Agency. Should agencies choose to use an RMC, the RMC should be chaired by the Agency Chief Operating Officer (COO) or a senior official with responsibility for the enterprise. In cabinet-level Agencies this is the Deputy Secretary.

To support this work, some agency governance structures are beginning to include a Chief Risk Officer (CRO), or equivalent function who champion agency-wide efforts to manage risk within the Agency and advise senior leaders on the strategically-aligned portfolio view of risks at the Agency. A CRO may serve as a strategic advisor to the COO and other staff on the integration of enterprise risk management practices into the day-to-day business operations and decision-making. CROs generally work with business unit managers within their organizations to identify

issues in a timely manner to allow for proactive management of the program and to facilitate informed, data-driven decision-making.

Regardless of the governance structure developed, agency governance should include a process for considering risk appetite and tolerance levels. The concept of “risk appetite” is key to achieving effective ERM, and is essential to consider in determining risk responses. Although a formally documented risk appetite statement is not required, agencies must have a solid understanding of their risk appetite and tolerance levels in order to create a comprehensive enterprise-level risk profile. Risk appetite can be considered qualitatively and/or quantitatively and should be factored into the process of balancing risks with opportunities. Additionally, risk appetite and tolerance levels should be evaluated on a regular basis and adjusted accordingly to meet the needs of the organization.

See OMB Circular No. A-11 Section 270.26, for a discussion of the broader risk management roles the RMC should fulfill with respect to strategic reviews.

## **B. Risk Profiles<sup>4</sup>**

Agencies must maintain a risk profile. The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives. The risk profile differs from a risk register in that it is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks. The risk profile must consider risks from a portfolio perspective and be approved by an Agency’s RMC or equivalent. Additionally, the profile must identify sources of uncertainty, both positive (opportunities) and negative (threats).

The development of an Agency risk profile:

- encourages open and candid conversations about risks facing an organization at all levels;
- facilitates the ranking of risk priorities (in particular to identify and escalate the most significant risks of which senior management should be aware);
- captures the reasons for decisions made about risk tolerances;
- facilitates recording of the way in which it is decided to address risk;
- allows leadership at all levels to understand the overall risk profile and how their areas of particular responsibility fit into it; and
- facilitates the review and regular monitoring of risks.

---

<sup>4</sup> Based on The Orange Book, Management of Risk – Principles and Concepts, October 2004, HM Treasury.

**Agencies have discretion in terms of the appropriate content and format for their risk profiles;** however, in general risk profiles should include the following seven components:

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

Each of these seven components is illustrated in the table below, and further descriptions of each component, including guidance for each, follows the table. In completing their risk profiles, Agencies may consider reviewing and incorporating results from existing documentation such as GAO and OIG Audit Findings, OIG's Annual Report on Top Performance and Management Challenges, FFMIA/FMFIA documentation, Employee Viewpoint Survey Results, external media, etc.

Agencies should adhere to the general guidance provided for these components when making modifications to the content and format of their risk profiles. See Sections C1 through C7 following the table below.

**Table 1 Illustrative Example of a Risk Profile**

<b>STRATEGIC OBJECTIVE – Improve Program Outcomes</b>								
	Inherent Assessment		Current Risk Response	Residual Assessment		Proposed Risk Response	Owner	Proposed Risk Response Category
Risk	Impact	Likelihood		Impact	Likelihood			
Agency X may fail to achieve program targets due to lack of capacity at program partners.	High	High	REDUCTION: Agency X has developed a program to provide program partners technical assistance	High	Medium	Agency X will monitor capacity of program partners through quarterly reporting from partners	Primary – Program Office	Primary – Strategic Review
<b>OPERATIONS OBJECTIVE – Manage This Risk of Fraud in Federal Operations</b>								
Contract and Grant fraud.	High	Medium	REDUCTION: Agency X has developed procedures to ensure contract performance is monitored and that proper checks and balances are in place.	High	Medium	Agency X will provide training on fraud awareness, identification, prevention, and reporting.	Primary – Contracting or Grants Officer	Primary – Internal Control Assessment
<b>REPORTING OBJECTIVE – Provide Reliable External Financial Reporting</b>								
	Inherent Assessment		Risk Response	Residual Assessment		Proposed Action	Owner	Proposed Action Category
RISK	Impact	Likelihood		Impact	Likelihood			
Agency X identified material weaknesses in internal control.	High	High	REDUCTION: Agency X has developed corrective actions to provide program partners technical assistance.	High	Medium	Agency X will monitor corrective actions in consultation with OMB to maintain audit opinion.	Primary – Chief Financial Officer	Primary – Internal Control Assessment
<b>COMPLIANCE OBJECTIVE – Comply with the Improper Payments Legislation</b>								
Program X is highly susceptible to significant improper payments.	High	High	REDUCTION: Agency X has developed corrective actions to ensure improper payment rates are monitored and reduced.	High	Medium	Agency X will develop budget proposals to strengthen program integrity.	Primary – Program Office	Primary – Internal Control Assessment and Strategic Review



## **B1. Identification of Objectives**

Risk must be analyzed in relation to achievement of the strategic objectives established in the Agency strategic plan (See OMB Circular No. A-11, Section 230), as well as risk in relation to appropriate operational objectives. Specific objectives must be identified and documented to facilitate identification of risks to strategic, operations, reporting, and compliance. This process assists in the identification of formal internal controls and compliance with the FMFIA, as discussed in Section III. In summary, the risk profile must include the following objectives:

- **Strategic Objectives:** relating to the strategic goals and objectives aligned with and supporting the Agency's Mission (See OMB Circular No. A-11, Section 230).
- **Operations Objectives:** relating to the effective and efficient use of the Agency's resources related to administrative and major program operations, including financial and fraud objectives (Refer to Section III, Establishing And Operating An Effective System Of Internal Control).
- **Reporting Objectives:** relating to the reliability of the Agency's reporting.
- **Compliance Objectives:** relating to the Agency's compliance with applicable laws and regulations.

In some cases there will be overlap across these categories, and agencies have discretion in terms of how to address this overlap. In addition, Agencies may find it useful to include additional subcategories of one or more objectives categories to facilitate communication on a narrower topic. One of the most common subcategories includes reputational risk. Reputational risk damages the reputation of an Agency or component of an Agency to the point of having a detrimental effect capable of affecting the Agency's ability to carry out mission objectives. Examples of reputational risk include the loss of confidence and trust, which stakeholders have in an organization to deliver operational services, or the loss of an Agency's financial statement opinion. Agencies may use their discretion in determining how to incorporate additional subcategories into their risk profile.

## **B2. Identification of Risk**

Identifying risks is a critical step in building the Agency's risk profile. The identification of risk can be separated into two distinct phases:

1. Initial risk identification (for an Agency which has not previously identified its risks in a structured way, or for a new component of an Agency, or perhaps for a new project or activity within an Agency); and

2. Continuous risk identification (which is necessary to identify new or emerging risks, and/or changes in existing risks).

The identification of risk is a continuous and ongoing process. 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.

Assessing risk is the next critical step in building the Agency's risk profile, which includes three important principles:

1. Ensure that there is a clearly structured process in which both likelihood and impact are considered for each risk;
2. record the assessment of risk in a way which facilitates monitoring and the identification of risk priorities; and
3. be clear about the difference between inherent and residual risk.

Some risk is unavoidable and beyond an organization's ability to reduce to a tolerable level. Nevertheless, the organization should make contingency plans and manage risks against those plans. For example, many organizations have to accept that risk arises due to natural disaster situations that they cannot control.

### **B3. Inherent Risk Assessment**

Inherent risk is the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations. The impact on the Agency's ability to achieve its objectives if the risk occurred can be ranked by appropriate categories, as can the likelihood that each significant risk might occur. While agencies can design their own appropriate categories, for the purposes of this guidance the following illustrative definitions can be used:

#### **Impact**

- High: the impact could preclude or highly impair the entity's ability to achieve one or more of its objectives or performance goals;
- Medium: the impact could significantly affect the entity's ability to achieve one or more of its objectives or performance goals; and
- Low: the impact will not significantly affect the entity's ability to achieve one or more of its objectives or performance goals.

#### **Likelihood**

- High: the risk is very likely or reasonably expected to occur;
- Medium: the risk is more likely to occur than unlikely; and
- Low: the risk is unlikely to occur.

#### **B4. Current Risk Response**

The action taken to manage the risk. It could involve one or more of the following:

- **Acceptance:** No action is taken to respond to the risk based on the insignificance of the risk; or the risk is knowingly assumed to seize an opportunity.
- **Avoidance:** Action is taken to stop the operational process, or the part of the operational process, causing the risk.
- **Reduction:** Action is taken to reduce the likelihood or impact of the risk.
- **Sharing:** Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.<sup>5</sup>

Risk responses take many forms, including: avoidance of risk by development of a legislative proposal; reduction of risk by proposing to increase funding for the activity; acceptance of the risk of adopting a new technology in order to provide better services to customers. Formulation of risk responses should consider the organization's risk appetite and tolerance levels. The development of risk responses should be used to inform decision-making through existing management processes including the strategic reviews, development of the legislative and policy agenda, operational planning, and budget formulation.

As part of developing the risk profile, management must determine those risks for which the appropriate response includes implementation of formal internal control activities as described in Section III of this guidance and which conform to the standards published by GAO in the [Green Book](#). These include those risks that meet each of the following criteria:

- The Agency is working to reduce exposure to the risk.
- The objective is related to reporting, compliance, or operations, including both administrative operations and the major operational components of programs.
- The risk is identified in the Agency risk profile as at least medium impact and medium likelihood (i.e., the risk is greater than low).
- Public reporting on the risk will not negatively impact services provided to the public, national security, or agency operations.
- Control objectives can be clearly specified.

---

<sup>5</sup> Based on definitions outlined by GAO in the [Green Book](#).

## **B5. Residual Risk Assessment**

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

## **B6. Proposed Action**

Additional action proposed to further reduce the exposure remaining after the risk mitigation actions have been taken, for consideration by senior management, Proposed risk responses should use the same standards applied to the current risk response, as described above, including the identification of risks for which implementation of formal internal control activities is appropriate.

## **B7. Proposed Risk Response Category**

Identification of the existing management process that will be used to implement and monitor proposed actions. Those proposed actions that will be discussed with OMB as part of the annual Strategic Review must be identified (See [OMB Circular No. A-11, Section 270](#)), as well as proposed actions to be considered during formulation of the President's Budget. In particular, the RMC or other equivalent governance body, must categorize actions for the adoption of formal internal control activities (as described in Section III of this guidance and which conform to the standards published by GAO in the [Green Book](#)), when the criteria identified above under Current Risk Responses have been met.

**Risk Profile Disclosure.** As explained above, the development of agency risk profiles requires candor, subjective evaluations, and frank discussions in identifying the likelihood and severity of internal vulnerabilities. In addition, risk profiles serve to inform the development of agency strategic plans as well as the President's Budget. As such, agency risk profiles will often contain pre-decisional, deliberative, confidential, or sensitive information. Agencies are encouraged to consult with their Office of General Counsel if there are questions regarding the disclosure of such information.

## **C. Implementation**

The management of risk must be regularly reviewed to monitor whether or not the risk profile has changed and to gain assurance that risk management is effective or if further action is necessary. In addition, processes must be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks have changed, to report significant changes that adjust risk priorities, and deliver assurance on the effectiveness of control. In addition, the overall risk management process must be subjected to regular review to

deliver assurance that it remains appropriate and effective. At a minimum, management's risk management review processes must<sup>6</sup>:

- ensure that all aspects of the risk management process are reviewed at least once a year;
- ensure that risks themselves are subjected to review with appropriate frequency; and
- make provisions for alerting the appropriate level of management to new or emerging risks, as well as changes in already identified risks, so that the change can be appropriately addressed.

Federal agencies have diverse missions, and are at different levels of maturity in terms of their capacity to fully implement ERM. The Agency's approach for developing risk profiles and implementing ERM should be refined and improved each year. This guidance recognizes that not all components of an ERM process are fully operationalized in the initial years, and agency leadership must set priorities in terms of implementation. Unless otherwise approved by OMB, agencies must meet the following deadlines:

**Figure 3 ERM Development and Implementation Deadlines**

Deliverable	Due Date – No later than:	Description
ERM Implementation Approach	<i>As soon as practicable, prior to June Initial Risk Profile deliverable</i>	Agencies are encouraged (not required) to develop an approach to implement Enterprise Risk Management (ERM) which may include: <ul style="list-style-type: none"> <li>• planned risk management governance structure,</li> <li>• Process for considering risk appetite and risk tolerance levels,</li> <li>• methodology for developing a risk profile,</li> <li>• general implementation timeline, and plan for maturing the comprehensiveness and quality of the risk profiles over time.</li> </ul>
Initial Risk Profile	<i>June 2, 2017*</i>	Agencies must complete their initial risk profiles in coordination with the agency Strategic Reviews. Key findings should be made available for discussion with OMB by June 2, 2017* as part of the Agency Strategic Review meetings and/or FedSTAT. The final determination on information to be shared with OMB will be provided in early 2017. This initial Risk Profile will inform the development of each Agency's new strategic plan and the President's FY 2019 Budget.
Integration with Management Evaluation of Internal Control	<i>September 15, 2017</i>	For those risks for which formal internal controls have been identified as part of the Initial Risk Profile in FY 2017, all agencies must present assurances on internal control processes in the FY 2017 Agency Financial Report (AFR) or the Performance and Accountability Report (PAR), along with a report on identified material

<sup>6</sup> Based in part on The Orange Book, Management of Risk – Principles and Concepts, October 2004, HM Treasury.

		weaknesses and corrective actions. Until an agency has fully implemented an ERM approach to risk management, it may continue to provide the existing risk assurance statements to their OIG and/or private accounting firms, as appropriate.
Updated Risk Profile	<i>Annually by June 3*</i>	No less than annually, all agencies must prepare a complete risk profile and include required risk components and elements required by this guidance.  CFO Act agencies, at a minimum, must complete their risk profiles in coordination with the agency Strategic Review. For these Agencies, key findings should be made available for discussion with OMB by June 3 <sup>rd</sup> * as part of the agency Strategic Review meetings and/or FedStat. The final determination on information to be shared with OMB will be provided in advance of these discussions. The Risk Profile will help to inform changes to strategy, policy, operations, and the President's Budget.

\* OMB Circular No. A-11, Part 6, is the authoritative policy guidance on deadlines for the Summary of Findings from the agency Strategic Reviews, including the timing of submissions to OMB. Agencies should consult OMB Circular No. A-11 as each prepares materials.

After initial implementation, the agency's risk profile must be discussed each year with OMB as a component of the summary of findings from the Agency strategic review and FedSTAT (See OMB Circular No. A-11, Section 270). For those objectives for which formal internal control activities have been identified as part of the Risk Profile, assurances on internal control processes must be presented in the Agency Financial Report (AFR) or Performance and Accountability Report (PAR), along with a report on identified material weaknesses and corrective actions.

#### **D. Role of Auditors in Enterprise Risk Management**

Management is responsible for Enterprise Risk Management systems. Internal or external auditors conduct independent and objective audits, evaluations, and investigations of an Agency's programs and operations, which includes aspects of the internal control and risk management systems. Management uses the results of such evaluations, including accompanying findings and recommendations, to monitor the design or operating effectiveness of these systems at a specific time or of a specific function or process. Auditors are also responsible for keeping management informed about risks that it detects, including fraud risks, and thereby provides information to management for use in the identification and assessment of risks. Management and external auditors might have different interpretations of risks based on their respective roles and responsibilities. The agency risk function should seek to coordinate their roles so that the independence and scope of the external auditor's role is preserved while ensuring the continuing flow of risk information to the risk management function.

### III. ESTABLISHING AND OPERATING AN EFFECTIVE SYSTEM OF INTERNAL CONTROL

The FMFIA requires the GAO to prescribe standards of internal control in the Federal Government, more commonly known as the [Green Book](#). These standards provide the internal control framework and criteria Federal managers must use in designing, implementing, and operating an effective system of internal control. The [Green Book](#) defines internal control as a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity are achieved. These objectives and related risks can be broadly classified into one or more of the following categories:

- Operations: Effectiveness and efficiency of operations;
- Reporting: Reliability of reporting for internal and external use; and
- Compliance: Compliance with applicable laws and regulations.

A subset of the categories of objectives are the safeguarding of all assets. Management designs an internal control system to provide reasonable assurance regarding the prevention or prompt detection and correction of unauthorized acquisition, use, or disposition of an entity's assets.

FMFIA also requires OMB, in consultation with GAO, to establish guidelines for agencies to evaluate their systems of internal control to determine FMFIA compliance. Instead of considering internal control as an isolated management tool, agencies must integrate their efforts to meet the requirements of the FMFIA with the Enterprise Risk Management (ERM) requirements discussed in Section II. Thus, internal control is an integral part of the entire cycle of strategic planning, goal and objective setting, budgeting, program management, accounting, and auditing. It must support the effectiveness and the integrity of every step of the process and provide continual feedback to management.

Federal managers must carefully consider the appropriate balance between risk, controls, costs, and benefits in their mission-support operations. Too many controls can result in inefficiencies, while too few controls might increase risk to an unacceptable level.

Management's responsibility is to develop and maintain effective internal control that is consistent with its established risk appetite and risk tolerance levels. In addition, management is responsible for establishing and integrating internal control into its operations in a risk-based and cost beneficial manner, in order to provide reasonable assurance that the entity's internal control over operations, reporting, and compliance is operating effectively.

Achieving the objectives of external reporting and compliance, which are based largely on laws, rules, regulations, and standards established by Congress, GAO, and OMB, depends on how activities within the Agency's control are performed. Generally, management and oversight bodies have greater discretion in setting internal reporting objectives that are not driven by external parties. However, Agency's may choose to align its internal and external reporting objectives to allow internal reporting to better support the Agency's external reporting.

Achievement of some operations objectives – such as certain aspects of program outcomes or maintaining safe operations – are not always within the Agency’s control. An effective internal control system increases the likelihood that an entity achieves its objectives. However, no matter how well designed, implemented, or operated, an internal control system cannot provide absolute assurance that all of an organization’s objectives are met. Factors outside the control or influence of management can affect the entity’s ability to achieve all of its objectives. For example, a natural disaster can affect an organization’s ability to achieve its objectives. Therefore, once in place, effective internal control provides reasonable, not absolute, assurance that an organization achieves its objectives.

The [Green Book](#) is organized by five components of internal control as shown in the exhibit below. In addition, the five components of internal control contain 17 required principles and each principle has important attributes which explain the principles in greater detail.

*Table 2 Summary of Green Book Components and Principles of Internal Control*

Components of Internal Control	Principles
Control Environment	<ol style="list-style-type: none"> <li>1. Demonstrate Commitment to Integrity and Ethical Values</li> <li>2. Exercise Oversight Responsibility</li> <li>3. Establish Structure, Responsibility and Authority</li> <li>4. Demonstrate Commitment to Competence</li> <li>5. Enforce Accountability</li> </ol>
Risk Assessment	<ol style="list-style-type: none"> <li>6. Define Objectives and Risk Tolerances</li> <li>7. Identify, Analyze, and Respond to Risk</li> <li>8. Assess Fraud Risk</li> <li>9. Analyze and Respond to Change</li> </ol>
Control Activities	<ol style="list-style-type: none"> <li>10. Design Control Activities</li> <li>11. Design Activities for Information Systems</li> <li>12. Implement Control Activities</li> </ol>
Information and Communication	<ol style="list-style-type: none"> <li>13. Use Quality Information</li> <li>14. Communicate Internally</li> <li>15. Communicate Externally</li> </ol>
Monitoring	<ol style="list-style-type: none"> <li>16. Perform Monitoring Activities</li> <li>17. Remediate Deficiency</li> </ol>

Federal managers must carefully consider the appropriate balance between controls and risk in their programs and operations. To emphasize, too many controls can result in inefficient and ineffective government; agency managers must ensure an appropriate balance between the strength of controls and the relative risk associated with particular programs and operations. The benefits of controls should outweigh the cost. Agencies should consider both qualitative and quantitative factors when analyzing costs against benefits.

## **A. Governance.**

Agencies must have a Senior Management Council (SMC) to assess and monitor deficiencies in internal control. This SMC may be a subset of the Risk Management Council, however, agencies have discretion in determining the appropriate structure. A Senior Management Council may include the Chief Financial Officer, Chief Human Capital Officer, Chief Information Officer, Chief Information Security Officer, Chief Acquisition Officer, Senior



Agency Official for Privacy, Designated Agency Ethics Official, and Performance Improvement Officer and the managers of other program offices, must be involved in identifying and ensuring correction of systemic material weaknesses relating to their respective programs. Such councils generally recommend to the Agency head which significant deficiencies are deemed to be material weaknesses to the Agency as a whole, and must therefore be included in the annual FMFIA assurance statement and reported in the Agency's Annual Financial Report (AFR) or Performance Accountability Report (PAR). This council should be responsible for overseeing the timely implementation of corrective actions related to material weaknesses. Such a council is also useful in determining when sufficient action has been taken to declare that a significant deficiency or material weakness has been corrected (though the final official determination likely resides with the Agency Head and the OIG). The SMC should also include Senior Assessment Teams to lead assessments related to the objective of internal control over reporting (See Appendix A to OMB Circular No. A-123, *Internal Control Over Reporting*).

## **B. Establish Entity Level Control**

Establishing Entity Level Control (ELC) is another primary step in operating an effective system of internal control. The [Green Book](#) defines ELCs as controls that have a pervasive effect on an entity's internal control system and pertain to multiple components. ELCs are mostly within the Control Environment, Risk Assessment, Information and Communication, and Monitoring components of the [Green Book](#). Control Activities are also considered a component of ELC and provide a link to an Agency's processes as described in Section C below. Entity-level controls also include controls related to the entity's use of service organizations or management override of internal control and fraud.

### **B1. Service Organizations**

The [Green Book](#) provides internal control considerations for service organizations (shared service providers (SSP) are one example). Service organization internal control considerations include management's responsibility for the performance of third party provided processes, establishing "user controls" at the Agency receiving services, and service organization oversight.

- **Management's Responsibility for the Processes Performed by Third Party Service Organizations.** Third party service providers perform activities for many agencies. Examples include, but are not limited to: accounting and payroll processing, employee benefit plan servicing, information technology services, protections for sensitive Agency data, acquisition or procurement services, security services, asset management, health care claims processing, and loan servicing. Agencies are ultimately responsible for the services and processes provided by third party service organizations as they relate to the Agency's ability to maintain internal control over operations, reporting, and compliance with laws and regulations.
- **Management's Responsibility for Establishing User Controls.** If the processes provided by the third party service organization is significant to an Agency's internal control objectives, then the Agency is responsible for establishing user Agency controls that complement the service organization's controls. Management still

retains overall responsibility and accountability for all controls related to the processes provided by the third party, and must monitor the process as a whole to make sure it is effective. Examples of user Agency controls include:

- **Input/ Output Controls:** In most third party provider situations, the Agency must have access to the information processed by a service organization. In some cases, this information enables the Agency to compare the service organization's results with the results of an independent source. For example, an Agency using a payroll service organization compares the data submitted to the service organization with reports or information received from the service organization after the data has been processed.
- **Performance Monitoring:** Agencies must have a process for monitoring the service organization's performance in relation to various metrics, as typically defined in a service-level agreement. Most of these metrics must be tailored to specific operations. For example, agencies regularly review the security, availability, and processing integrity of service-level agreements.
- **Process Controls:** In some third party provider situations, the Agency's user controls are closely tied to the service organization's processes and provide direct assurance over their operation. For example, an Agency that has its IT development provided by a third party service organization chooses to document, track, approve, and test all application changes internally, thus retaining significant control over the IT development process.
- **Management's Responsibility for Oversight of Service Organizations.** The extent of an Agency's oversight of a service organization depends on the nature of the contract or agreement terms and conditions. The use of a third party provider needs to be considered for management's oversight and assessment of internal control based on risk and when the activity is significant to the Agency's achievement of internal control objectives of operations, reporting, or compliance. Examples of services provided by the service organization that warrant oversight include: maintenance of a user Agency's financial reporting and accounting records; safeguarding of a user Agency's assets; services that involve personally identifiable information (PII); investments for employee benefit plans; mortgage services from servicers that service mortgages for others; or application services for technology environments that support operations.
- **Service Organization Responsibility.** Service Organizations are responsible for providing assurances to their customers and assisting customers in understanding the relationship between the service provider's controls and the customer's user controls. Together, service organizations and customers manage the risks of third party provider activities typically through a Service Organization Control (SOC) 1 Type 2

Report (more technically referred to as a Statement on Standards for Attestation Engagement No. 16 report<sup>7</sup>). SOC 1 report considerations include:

- Ensuring the SOC report adequately addresses the relevant internal control objectives.
- Determining the extent and adequacy of internal control testing performed on the operating effectiveness of internal controls throughout a specified period.
- Ensuring the SOC Report(s) cover a substantial portion of the fiscal year and bridge or roll forward letters are considered.
- Reviewing the SOC report opinion (e.g., Unmodified) and determining what impact any internal control deficiencies included in the SOC report have on the related control objectives.
- Evaluating complementary user entity controls included in the SOC 1 report to determine that the appropriate controls are in place to support the activities of the service provider.
- Considering any complementary subservice organization controls included in the SOC 1 report and the effectiveness of controls at subservice organizations.

## **B2. Managing Fraud Risks in Federal Programs**

The [Green Book](#) defines fraud as obtaining something of value through willful misrepresentation. Whether an act is fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person considers reasonable and necessary in operational practice given the facts and circumstances. This includes the misuse of authority or position for personal gain or for the benefit of another. Waste and abuse do not necessarily involve fraud or illegal acts.<sup>8</sup> Principle 8 of the [Green Book](#) requires management to consider the potential for fraud when identifying, analyzing, and responding to risks.

**OMB Circular No. A-123 Fraud Risk Profile Requirements.** Fraud jeopardizes Agency missions by diverting scarce resources from their intended purpose. A single case of fraud can undermine programmatic mission, disrupt services, and force management to expend valuable time, resources, and staff-hours to resolve and recover property lost due to fraud. Reputational risks of fraud can damage the perception of an Agency, impact employee morale, and create distrust by the public, further hindering their efforts to provide services to the public. To the extent that Federal managers can effectively mitigate and prevent fraud from occurring, it can

---

<sup>7</sup> Effective for service auditors' reports dated on or after May 1, 2017, service organization reports will be prepared under a new clarified attestation standard –AU-320.

<sup>8</sup> GAO Standards for Internal Control in the Federal Government, GAO-14-704G, Section 8.03.  
<http://www.gao.gov/assets/670/665712.pdf>.

save time and resources spent in investigating and prosecuting fraud, and recovering lost money and property, thus avoiding the “pay and chase model.”

Management has overall responsibility for establishing internal controls to manage the risk of fraud. This includes reporting to the Agency’s governance structure what actions have been taken to manage fraud risks and on the status of the Agency’s Risk Profile. The Agency’s Risk Profile as required by Section II of OMB Circular No. A-123 must include an evaluation of fraud risks and use a risk-based approach to design and implement financial and administrative control activities to mitigate identified material fraud risks. Refer to Appendix A of OMB Circular No. A-123, *Internal Control over Reporting*, for requirements related to reporting internal control objectives. The financial and administrative controls established through the Agency’s risk profile must also include:

- controls to address identified fraud risks related to payroll, beneficiary payments, grants, large contracts, information technology and security, asset safeguards, and purchase, travel and fleet cards;
- collecting and analyzing data from reporting mechanisms on detected fraud to monitor fraud trends and using that data and information to continuously improve fraud prevention controls; and
- using the results of monitoring, evaluation, and investigations to improve fraud prevention, detection, and response.

**GAO Framework for Managing Fraud Risks in Federal Programs.** To help managers to combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks and organized them into a conceptual framework called the Fraud Risk Management Framework (the Framework, [GAO-15-593SP](#)). 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 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, which are ongoing practices that apply to the following four components described below.

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

**Establishing Risk Tolerances in Disaster Situations.** Managers must balance their priorities to fulfill the program’s mission, such as effectively disbursing funds or providing services to beneficiaries, and taking actions to safeguard taxpayer dollars from improper use. For example, in disaster situations, fraud risks are higher than under normal circumstances because the need to provide services quickly can hinder the effectiveness of existing controls and creates additional opportunities for individuals to engage in fraud. As a result, managers face additional challenges balancing their mission to provide assistance quickly with implementing controls to address the increased risk of fraud.

GAO’s Fraud Framework calls for managers to determine risk tolerances when assessing fraud risks and to use that determination as part of the basis for developing responses to identified fraud risks, including specific controls to address the risks. Risk tolerance reflects managers’ willingness to accept a higher level of fraud risks and vary depending on the circumstances of the program. When determining risk tolerance in disaster situations, managers weigh the program’s operational objective of expeditiously providing assistance against the objective of lowering the likelihood of fraud, because activities to lower fraud risks—such as the risk that ineligible individuals submit fraudulent applications for benefits—causing delays in service. As a result, managers are willing to accept a somewhat higher risk of fraud than under normal circumstances in order to provide emergency assistance in a timely manner. GAO’s Fraud Framework provides a basis for managers to make decisions about how to respond to fraud risks, including determining the specific controls to design and implement, given managers’ defined risk tolerances.

Managers can find additional guidance provided in the Association of Government Accountants (AGA) Fraud Prevention Tool Kit useful when managing specific types of fraud risks in Federal programs. AGA’s [Fraud Prevention Tool Kit](#) provides current, state-of-the-art tools for Federal, state, local, and tribal government financial managers to use in preventing and detecting fraud.

## IV. ASSESSING INTERNAL CONTROL

Agency managers must continuously monitor, assess, and improve the effectiveness of internal control associated with those internal control objectives identified as part of their risk profile. This continuous monitoring, and other periodic evaluations, provide the basis for the Agency Head's annual assessment and report on internal control as required by the FMFIA.

### A. Documentation Requirements

Agency management must determine the appropriate level of documentation needed to support this assessment. The [Green Book](#) provides documentation requirements that are a necessary part of an effective internal control system. The level and nature of documentation vary based on the size of the entity and the complexity of the operational processes the entity performs. Management uses judgment in determining the extent of documentation that is needed. Documentation is required to demonstrate the design, implementation, and operating effectiveness of an entity's internal control system. The [Green Book](#) includes minimum documentation requirements as follows:

- If management's assessment determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component may be designed, implemented, and operated effectively.
- Management develops and maintains documentation of its internal control system.
- Management documents in policies the internal control responsibilities of the organization.
- Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues.
- Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis.
- Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis.

### B. Sources of Information

The Agency's assessment of internal control may be documented using a variety of information sources to include:

- Management documentation of its internal control system, policies, procedures, and knowledge gained from the daily operation of Agency programs and systems.
- Management reviews conducted (i) expressly for the purpose of assessing internal control, or (ii) for other purposes with an assessment of internal control as a by-product of the review.
- Annual performance plans, reports, strategic reviews and program evaluations relevant to internal control pursuant to the *GPRA Modernization Act* and OMB [Circular No. A-11](#), Section 200, Federal Performance Framework.

- Acquisition Assessments pursuant to OMB Memorandum: *Conducting Acquisition Assessments under OMB Circular No. A-123*, May 21, 2008.
- Management reviews and annual evaluations and reports related to information technology, information security, and information resources pursuant to the Federal Information Security Modernization Act of 2014 and OMB Circular No. A-130, *Responsibilities for Protecting Federal Information Resources*.
- Outputs of governance mechanisms for information technology resources published by the Agency, pursuant to the “CIO Authorities” described in the *Federal Information Technology Acquisition Reform Act (FITARA)*.
- Office of Government Ethics Program Reviews and other internal Agency ethics program reviews.
- Annual reviews and reports pursuant to the Improper Payments Information Act of 2002, as amended by the Improper Payments Elimination and Recovery Act of 2010 and the Improper Payments Elimination and Recovery Improvement Act of 2012.
- Program reviews conducted pursuant to OMB Circular No. A-129, *Policies for Federal Credit Programs and Non-Tax Receivables*.
- Single Audit Act Reports and program reviews conducted pursuant to the *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* for grant-making agencies.
- Antideficiency Act Reviews and Investigations.
- Independent audit reports including Office of Inspectors General Management Challenges and GAO High Risk Reports.
- Internal audit reports.
- Reports and other information provided by the Congressional committees of jurisdiction.
- Other reviews or reports relating to Agency operations or management controls.
- Assessments of internal control over financial reporting and reviews of financial management systems pursuant to Appendix A of OMB Circular No. A-123, *Internal Control Over Reporting*, Appendix B to OMB Circular No. A-123, *Improving the Management of Government Charge Card Program*, Appendix C to OMB Circular No. A-123, *Requirements for Effective Estimation and Remediation of Improper Payments*, or Appendix D to OMB Circular No. A-123, *Compliance with the Federal Financial Management Improvement Act*.

Use of information should take into consideration the completeness of the assessment and whether the process included an evaluation of internal control. Agency management should avoid duplicating reviews that assess internal controls, and should coordinate their efforts with other evaluations to the extent practical.

### **C. Identification of Deficiencies**

Agency managers and employees should identify deficiencies in internal control from the sources of information described above and the results of their assessment process. The assessment process must include an assessment of compliance with each of the [Green Book](#) components and principles. In addition, the identification of deficiencies must include all management and operational functions and processes that support mission delivery. Agency employees and managers report control deficiencies, at a minimum to the next supervisory level,



which allows the chain of command structure to determine the relative importance of each deficiency. Reporting of deficiencies should also include reporting deficiencies to the Agency's Inspector General. Definitions of control deficiencies, significant deficiencies, and material weaknesses are provided in Section VI.

Agency managers and staff are encouraged to identify control deficiencies, as this reflects positively on the Agency's commitment to recognizing and addressing management problems. Failing to report a known material weakness or significant deficiency reflects adversely on the Agency and continue to place the Agency's mission support operations at risk. Agencies must carefully consider whether systemic weaknesses exist that adversely affect internal control across organizational or program lines.

#### **D. Internal Control Evaluation Approach**

Management is responsible for evaluating whether a system of internal control reduces the risk of not achieving the entity's objectives related to operations, reporting, or compliance to an acceptable level. In evaluating internal control, management should follow a risk-based assessment approach:<sup>9</sup>

1. **Conduct an Assessment of Internal Control.** Management must conduct an evaluation of internal controls for each of the [Green Book's](#) principles for each of the entity objectives.
2. **Prepare a Summary of Internal Control Deficiencies.** Management should leverage an aggregated or summary log of all identified internal control deficiencies from the sources of information listed in Section B above and the results of their assessment process. The log may support the evaluation of the [Green Book's](#) Internal Control Components and Principles.
3. **Conclude on Internal Control Principle Evaluation.** Management must summarize its determination of whether each principle is designed, implemented, and operating effectively. That determination is a function of management judgment based on:
  - a. the applicability of the principle to the Agency's circumstances,
  - b. whether the Agency has actually been able to implement, perform, and apply the principle,
  - c. any internal control deficiency that may result,
  - d. the extent of compensating internal controls within the principle, and
  - e. the extent to which the remaining risk impacts on the Agency's ability to achieve its objectives and meet its mission and goals.

---

<sup>9</sup> Section based on [COSO](#), Internal Control – Integrated Framework, Illustrative Tools for Assessing Effectiveness of a System of Internal Control (New York: American Institute of Certified Public Accountants, 2013).



Evaluation of whether each principle is designed, implemented, and operating effectively must be of the “yes/no” type.

4. **Conclude on Internal Control Component Evaluation.** Management must also summarize its determination of whether each component is designed, implemented, and operating effectively. Similar to item three above, evaluation of internal control components is a function of management judgment and qualitative determinations. If an internal control principle is not designed, implemented, and operating effectively, management is unable to conclude that the internal control component is operating effectively.
5. **Conclude on Overall Assessment of a System of Internal Control.** Management must summarize its determination of whether each of the [Green Book's](#) components and principles are designed, implemented, and operating effectively and components are operating together in an integrated manner. In addition, management must determine the severity of internal control deficiencies or combination of deficiencies when aggregated across the components. If one or more internal control components are not operating effectively, a material weakness must be reported.

The following table illustrates how internal control principles within the control environment component roll up into the determination of whether the component is designed, implemented, and operating effectively, in addition to the overall assessment of a system of internal control. Examples below include illustrative summaries of control deficiencies.

**Table 3 Illustrative Internal Control Evaluation – Control Environment**

Illustrative Internal Control Evaluation – Control Environment	
Principle	Control Deficiency Summary
Principle 1: Demonstrate Commitment to Integrity and Ethical Values	The Agency’s ethics training program is not sufficient to make all employees aware of the importance of adhering to the executive branch employee standards of conduct.
	The Agency does not have processes in place to detect and mitigate potential employee conflicts of interest.
	Management concludes the principle is not designed, implemented, and operating effectively.
Principle 2: Exercise Oversight Responsibility	Internal control deficiency noted because the Senior Management Council’s review of risk assessments and remediation plans are not documented.
	Management concludes that the principle is designed, implemented, and operating effectively despite internal control deficiencies based on an evaluation of the severity of deficiencies and that compensating controls are in place.
Principle 3: Establish Structure, Responsibility and Authority	Internal control deficiency noted because oversight and control structures have not evolved to keep up with changes in operations.
	Management concludes that the principle is designed, implemented, and operating effectively as the deficiency noted only affect a small portion of the Agency.
Principle 4: Demonstrate Commitment to Competence	No internal control deficiencies noted.
	Management concludes that the principle is designed, implemented, and operating effectively.
Principle 5: Enforce Accountability	Internal control deficiencies noted because management, with oversight from the Senior Management Council, does not take necessary corrective actions.
	Management concludes that the principle is not designed, implemented, and operating effectively.

The following table is an illustrative example of the results of management’s assessment of the control environment component:

**Table 4 Principle and Component Evaluation**

Principle Evaluation		
Principle	Designed & Implemented (Yes/No)	Operating Effectively
1) Demonstrate Commitment to Integrity and Ethical Values	No	Ineffective
2) Exercise Oversight Responsibility	Yes	Effective with internal control deficiencies and compensating controls noted
3) Establish Structure, Responsibility and Authority	Yes	Effective with internal control deficiencies and compensating controls noted

4) Demonstrate Commitment to Competence	Yes	Effective
5) Enforce Accountability	No	Ineffective

Component Evaluation		
Component	Designed & Implemented (Yes/No)	Operating Effectively
Control Environment	No	Ineffective

In the table above, management concludes the Control Environment Component is not designed, implemented, and operating effectively since two principles are not designed, implemented, and operating effectively due to the identified deficiencies from the summary log. Each principle supports the design, implementation, operational effectiveness of the associated component. If one principle is ineffective, management is unable to conclude that the component is effective.<sup>10</sup> In the table below, since management concluded that the Control Environment is not operating effectively, it must conclude that the overall system of internal control was not operating effectively and an entity-level control material weakness must be reported.

*Table 5 Overall Assessment of a System of Internal Control*

Overall Assessment of a System of Internal Control		
System Evaluation	Designed & Implemented (Yes/No)	Operating Effectively
Control Environment	No	Ineffective
Risk Assessment	Yes	Effective
Control Activities	Yes	Effective
Information and Communication	Yes	Effective
Monitoring	Yes	Effective
Are all Components operating together in an integrated manner?	No	Ineffective

Overall Evaluation of a System of Internal Control	
Overall Evaluation	Operating Effectively
Is the overall system of internal control effective?	No

<sup>10</sup> See Green Book OV3.03, Factors of Effective Internal Control

## **V. CORRECTING INTERNAL CONTROL DEFICIENCIES**

### **A. Importance of Correcting Internal Control Deficiencies**

Correcting control deficiencies is an integral part of management accountability and must be considered a priority by the Agency. An Agency's ability to correct control deficiencies is an indicator of the strength of its internal control environment. Effective remediation of control deficiencies is essential to achieving the objectives of the FMFIA, and uncorrected or longstanding control deficiencies must be considered in determining the overall effectiveness of internal control. The corrective action process provides the mechanism for management to present a comprehensive plan for addressing the risk associated with a control deficiency.

### **B. Corrective Action Plan Requirements**

Agencies should perform a root-cause analysis of the deficiency to ensure that subsequent strategies and plans address the root of the problem and not just the symptoms. Identifying and developing an understanding of the root cause of control deficiencies is management's responsibility. Management should incorporate IG and GAO audit findings as part of its identification process; however, auditors are not responsible for identifying root causes of control deficiencies. As a result, reliance on audit findings or recommendations alone may lead to incomplete corrective actions. Management should also consider alternative risk mitigation strategies and perform cost-benefit analysis to determine the best or most cost-effective solution.

A summary of the corrective action plans for material weaknesses that have not been fully mitigated at the time of reporting must be included in the Agency's AFR, PAR, or other management report. Also see Section VI for reporting on material weaknesses. The summary discussion must include a description of the material weakness, status of corrective actions, and timeline for resolution.

Management must maintain more thoroughly detailed corrective action plans internally, which must be made available for OMB and audit review. Management's process for resolution and corrective action of identified internal control deficiencies must:

- Communicate corrective actions to the appropriate level of the Agency and delegate authority for completing corrective actions to appropriate personnel.
- Determine the resources required to correct a control deficiency. The corrective action plan must indicate the types of resources needed (e.g., additional personnel, contract support, training, etc.), including non-financial resources, such as Senior Leadership support for correcting the control deficiency.
- Include critical path milestones that affect the overall schedule and performance of the corrective actions needed to resolve the control deficiency. Critical path milestones must lead to a date certain of the correction of the control deficiency.
- Require prompt resolution and internal control testing to validate the correction of the control deficiency.
- Ensure that accurate records of the status of the identified control deficiency are maintained and updated throughout the entire process.

- Ensure that the corrective action plans are consistent with laws, regulations, and Agency policy.
- Ensure that performance appraisals of appropriate officials reflect effectiveness in resolving or implementing corrective action for identified material weaknesses.
- Fully disclose uncorrected internal control weaknesses and highlight those that are material.

A determination that a control deficiency has been corrected should be made by the Senior Accountable Official only when sufficient corrective actions have been taken and validated. This determination must be in writing, supported by appropriate documentation, and made available for review by appropriate officials, e.g., the Agency's Senior Management Council or equivalent.

### **C. Audit Follow Up and Cooperative Audit Resolution and Oversight Initiatives**

As managers consider Office of Inspectors General (OIG), GAO, and other investigative audit reports in identifying and correcting internal control deficiencies, they must be mindful of the statutory requirements included in the Inspector General Act, as amended, and OMB Circular No. A-50, *Audit Follow-up*. Management has a responsibility to complete action, in a timely manner, on audit recommendations on which agreement with the OIG has been reached. Management must make a decision regarding OIG audit recommendations within a six-month period after issuance of the audit report and implement management's decision within one year to the extent practicable.

Some agencies use cooperative audit resolution and oversight initiatives (CAROI)<sup>11</sup> to complement oversight of corrective actions and internal control efforts. In addition, the Uniform Grant Guidance encourages agencies to use cooperative audit resolution mechanisms as part of audit follow-up techniques that promote prompt corrective actions by improving communication, fostering collaboration, promoting trust, and developing a common understanding of audit findings to improve Federal program outcomes. The AGA has conducted research and has developed a framework to implement CAROI at Federal agencies. The AGA provides, "the CAROI is a tool for achieving: 1) alternative and creative approaches to resolving audit findings and their underlying causes, and 2) greater success in attaining program goals at all levels of government through the constructive use of monitoring and technical assistance (i.e., oversight activities)." While the establishment of a CAROI is not a requirement of this document, a CAROI or similar construct is encouraged.

---

<sup>11</sup> <https://www.agacgfm.org/AGA/ToolsResources/documents/CAROI.pdf>.

## **VI. REPORTING ON INTERNAL CONTROLS**

### **A. Annual Assurance Statement.**

The assurance statement and summary information related to Section 2 and Section 4 of the FMFIA must be provided in a single report section of the annual AFR, PAR, or other management report labeled "Analysis of Entity's Systems, Controls and Legal Compliance." The section must include the annual assurance statement, a summary of the Agency's process for assessing internal control effectiveness and resulting material weaknesses and corrective action plans as of September 30 of a given fiscal year.<sup>12</sup> The assurance statement is an accountability statement so only essential information must be included. Table 5 provides a summary of internal control reporting requirements, and Exhibits 1, 2, and 3 provide illustrative examples of assurance statements.

### **B. Reporting Pursuant to Integration of Enterprise Risk Management and Internal Control**

Management has discretion in determining the scope of operations, reporting, and compliance objectives based on the Agency's risk profile as described in Section II of this document. Agencies are required to provide assurances on their process to identify risks and establish controls or integrate existing controls to the identified risk. Some of these internal control systems may have been operating effectively prior to integration of these risks. These assurances should be built out over time following a maturity model approach and reported in the AFR along with a report on identified material weaknesses and corrective actions. Until an Agency has fully implemented an ERM approach to risk management they may continue to provide the existing risk assurance statements to their OIG and/or private accounting firms.

### **C. Reporting Pursuant to OMB Circular No. A-123, Appendix A**

Appendix A of OMB Circular No. A-123 provides a methodology for agency management to assess, document and report on internal controls over reporting. This document also encourages an integrated approach to assess the internal controls over reporting considering the current legislative and regulatory environment in which Federal entities operate. Management's assessment of internal control over external financial reporting must follow the assessment methodology provided in Appendix A to Circular No. A-123, *Internal Control Over Reporting*.

---

<sup>12</sup> Agencies may use roll forward procedures for timing differences in different types of internal control assessments (e.g., timing differences between June 30 and September 30).

## **D. Reporting Pursuant to OMB Circular No. A-130, Appendix I**

Appendix I of OMB Circular No. A-130, *Responsibilities for Protecting and Managing Federal Information Resources*, establishes minimum requirements for Federal information security programs, assigns Federal Agency responsibilities for the security of information and information systems, and links Agency information security programs and Agency management control systems established in accordance with OMB Circular No. A-123. The appendix also establishes requirements for Federal privacy programs, assigns responsibilities for privacy program management, and describes how agencies must take a coordinated approach to implementing information security and privacy controls.

## **E. Reporting Pursuant to Section 2—31 U.S.C. 3512(d) (2)**

Section 2-31 U.S.C 3512(d) (2), commonly referred to as Section 2 of the FMFIA requires that the head of each Executive Agency annually submit to the President and the Congress (i) a statement on whether there is reasonable assurance that the Agency's controls are achieving their intended objectives; and (ii) a report on material weaknesses in the Agency's controls.

- **Statement of Assurance.** The statement of assurance represents the Agency head's informed judgment as to the overall adequacy and effectiveness of internal control within the Agency related to operations, reporting, and compliance. The statement must take one of the following forms:
  - unmodified statement of assurance (no material weaknesses or lack of compliance reported);
  - modified statement of assurance, considering the exceptions explicitly noted (one or more material weaknesses or lack of compliance reported); or
  - statement of no assurance (no processes in place or pervasive material weaknesses).

In deciding on the type of assurance to provide, the Agency head should consider information from the assessment process described in Section IV of this Circular, with input from senior program and administrative officials. Management is precluded from concluding that the Agency's internal control is effective (unmodified statement of assurance) if there are one or more material weaknesses. In support of a single assurance statement, a detailed summary of management assurances must also be provided in the "Other Information" section of the annual AFR, PAR, or other management report. The detailed assurances should mirror the single assurance statement and provide assurance over the effectiveness of internal controls in each supporting area of operations, reporting (including external financial reporting), and compliance.

The Agency Head must sign the statement of assurance.

## **F. Reporting Pursuant to Section 4—31 U.S.C. 3512(d) (2) (B)**

Section 4-31 U.S.C. 3512(d) (2) (B) commonly referred to as Section 4 of the FMFIA, requires CFO Act Agencies, a separate report on whether the Agency's financial management systems comply with government-wide requirements. These financial management systems requirements

are mandated by Section 803 (a) of the Federal Financial Management Improvement Act and Appendix D to OMB Circular No. A-123, *Compliance with the Federal Financial Management Improvement Act of 1996*. FFMIA Section 803(a) requirements include compliance with Federal Financial Management System Requirements, applicable Federal accounting standards, and the United States Standard General Ledger (USSGL) at the transaction level. If the Agency's systems do not comply with financial systems requirements, the statement must list the lack of compliance noted and discuss the Agency's plans for bringing its systems into compliance. Financial management systems include both financial and financially-related (or mixed) systems.

### **G. Government Corporations**

For government corporations, Section 306 of the Chief Financial Officers Act established a reporting requirement related to the internal controls for corporations covered by the Government Corporation Control Act. These corporations must submit an annual management report to the Congress. This report must include, among other items, a statement on control systems by the head of the management of the corporation consistent with the requirements of the FMFIA. The corporation is required to provide the President, the Director of OMB, and the Comptroller General a copy of the management report when it is submitted to the Congress.

### **H. Classified Matters**

The statement of assurance is made available to the public. However, relevant information that is specifically prohibited from disclosure by any provision of law, or specifically required by Executive Order to protect the interest of national defense or the conduct of foreign affairs, must not be included in the statement made available to the public. Descriptions of major vulnerabilities must be framed in such a way as to preclude an adverse party from exploiting the information.



**Table 6 Summary of OMB Circular No. A-123 Reporting Requirements**

Category	Definition	Reporting
Control Deficiency	<p>A control deficiency exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks.<sup>13</sup></p> <p>A deficiency in design exists when (1) a control necessary to meet a control objective is missing or (2) an existing control is not properly designed so that even if the control operates as designed, the control objective would not be met.<sup>14</sup></p> <p>A deficiency in implementation exists when a properly designed control is not implemented correctly in the internal control system.<sup>15</sup></p> <p>A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.<sup>16</sup></p>	Internal to the organization and not reported externally. Progress against corrective action plans must be periodically assessed and reported to agency management.
Significant Deficiency	A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance. <sup>17</sup>	Internal to the organization and not reported externally. Progress against corrective action plans must be periodically assessed and reported to agency management.

<sup>13</sup> Green Book OV3.08

<sup>14</sup> Green Book OV3.05

<sup>15</sup> Green Book OV3.05

<sup>16</sup> Green Book OV3.06

<sup>17</sup> Consistent with AU-C 260, *The Auditor's Communication With Those Charged With Governance*, the 2011 revision of *Government Auditing Standards* defines those charged with governance as the person(s) or organization(s) with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. This includes overseeing the financial reporting process, subject matter, or program under audit, including related internal controls.

Category	Definition	Reporting
Material Weakness	<p>A significant deficiency that the Agency Head determines to be significant enough to report outside of the Agency as a material weakness. In the context of the <a href="#">Green Book</a>, non-achievement of a relevant principle and related component results in a material weakness.<sup>18</sup></p> <p>A material weakness in internal control over operations might include, but is not limited to, conditions that:</p> <ul style="list-style-type: none"> <li>• impacts the operating effectiveness of Entity- Level Controls;</li> <li>• impairs fulfillment of essential operations or mission;</li> <li>• deprives the public of needed services; or</li> <li>• significantly weakens established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest.</li> </ul> <p>A material weakness in internal control over reporting is a significant deficiency, in which the Agency Head determines significant enough to impact internal or external decision-making and reports outside of the Agency as a material weakness.</p> <p>A material weakness in internal control over external financial reporting is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility<sup>19</sup> that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.</p> <p>A material weakness in internal control over compliance is a condition where management lacks a process that reasonably ensures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving Agency objectives.</p>	<p>Material weaknesses and a summary of corrective actions must be reported to OMB and Congress through the AFR, PAR, or other management reports. Progress against corrective action plans must be periodically assessed and reported to agency management.</p>

### ***Exhibit 1 Illustrative Unmodified Assurance Statement***

The [Agency] management is responsible for managing risks and maintaining effective internal control to meet the objectives of Sections 2 and 4 of the Federal Managers' Financial Integrity Act. The [Agency] conducted its assessment of risk and internal control in accordance with OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Based on the results of the assessment, the Agency can provide reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 20XX.

Head of the Agency Signature

### ***Exhibit 2 Illustrative Modified Assurance Statement***

The [Agency] management is responsible for managing risks and maintaining effective internal control to meet the objectives of Sections 2 and 4 of the Federal Managers' Financial Integrity Act. The [Agency] conducted its assessment of risk and internal control in accordance with OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Based on the results of the assessment, the Agency can provide reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 20XX, except for the following material weaknesses reported:

- [Insert brief description of each internal control material weakness;]

Head of the Agency Signature

---

<sup>18</sup> The Federal Information Security Modernization Act of 2014 no longer requires that a significant deficiency identified be reported as a material weakness for FMFIA.

<sup>19</sup> In this definition, a reasonable possibility exists when the likelihood of the event is reasonably possible or probable as those terms are used in AU-C 265, *Communicating Internal Control Related Matters Identified in an Audit*.

### ***Exhibit 3 Illustrative Statement of No Assurance***

The [Agency] management is responsible for managing risks and maintaining effective internal control to meet the objectives of Sections 2 and 4 of the Federal Managers' Financial Integrity Act. The [Agency] conducted its assessment of risk and internal control in accordance with OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Based on the results of the assessment, the Agency is unable to provide assurance that internal control over operations, reporting, and compliance was operating effectively due to the following material weaknesses:

- [Insert brief description of each internal control material weakness;]

Head of the Agency Signature

#### **I. Agencies Obtaining Audit Opinions on Internal Control**

Agencies may be required or may at their choice elect to receive an audit opinion on internal control over external financial reporting. These Agencies must provide a separate assurance statement for internal control over external financial reporting. The [Green Book](#) and OMB Circular No. A-123 provide adequate criteria for management's assessment of internal control and related management assurances. Public Company Accounting Oversight Board requirements for the private sector are not requirements of the Federal Government.

## VII. ADDITIONAL CONSIDERATIONS

### A. Managing Privacy Risks in Federal Programs

The Federal Government necessarily creates, collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of Personally Identifiable Information (PII) to carry out the missions mandated by Federal statute. The term PII, as defined by OMB, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency must perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.

Once the agency determines that an information system contains PII, the agency must then consider the privacy risks and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation. When considering privacy risks, the agency must consider the risks to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII. In particular, the agency must evaluate the sensitivity of each individual data element that is PII, as well as all of the data elements together. The sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, how the information will be processed and shared, and the ability to access the information. In addition, when determining the privacy and associated risks, the agency must also consider the volume of PII. A higher volume of PII about a single individual or multiple individuals may pose increased privacy or associated risks.

**Agency Privacy Programs.** In order to manage Federal information resources that involve PII, agencies must develop, implement, document, maintain, and oversee agency-wide privacy programs that include people, processes, and technologies. Agencies' privacy programs are led by the Senior Agency Official for Privacy (SAOP) and are responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks. Privacy programs' review of privacy risks should begin at the earliest planning and development stages of agency actions and policies that involve PII, and should continue throughout the life cycle of the information.

**Privacy Impact Assessments.** As a general matter, an agency must conduct a privacy impact assessment (PIA) under section 208(b) of the E-Government Act of 2002, absent an applicable exception under that section, when the agency develops, procures, or uses information

technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.<sup>20</sup> A PIA is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

A PIA is one of the most valuable tools Federal agencies use to ensure compliance with applicable privacy requirements and manage privacy risks. Agencies must conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle. In order to conduct a meaningful PIA, the agency's SAOP must work closely with the program managers, information system owners, information technology experts, security officials, counsel, and other relevant agency officials.

Moreover, a PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or PII life cycles. Rather, the privacy analysis must continue throughout the information system and PII life cycles. Accordingly, a PIA must be considered a living document that agencies are required to update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology.

In addition to serving as an important analytical tool for agencies, a PIA also serves as notice to the public regarding the agency's practices with respect to privacy and information technology. All PIAs must be drafted in plain language and must be posted on the agency's website, unless doing so would raise security concerns or reveal classified or sensitive information. Although PIAs are generally required by law, such as by the E-Government Act of 2002, agencies may also develop policies to require PIAs in circumstances where a PIA would not be required by law.

---

<sup>20</sup> See 44 U.S.C. § 3501 note. Section 208(b) of the E-Government Act requires agencies, absent an applicable exception under this section, to conduct a PIA before: (i) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that – (I) will be collected, maintained, or disseminated using IT; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

**Risk Management Framework.** Agencies' privacy programs have responsibilities under the Risk Management Framework.<sup>21</sup> The Risk Management Framework provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development life cycle. Agencies should refer to OMB Circular No. A-130 for more detailed guidance regarding the role of agencies' privacy programs under the Risk Management Framework.

## **B. Conducting Acquisition Assessments under OMB Circular No. A-123**

In May 2008, OMB's Office of Federal Procurement Policy (OFPP) issued guidelines, including an assessment template, to (1) establish a standard approach for assessing acquisition activities and programs; and (2) integrate these efforts into existing agency internal control processes and practices required by OMB Circular No. A-123. The template was adopted from the Government Accountability Office (GAO) Framework for Assessing the Acquisition Function at Federal Agencies (Framework) (GAO-05-218G) and consists of four interrelated areas, i.e. cornerstones, that are essential to an efficient, effective and accountable acquisition process: (1) organizational alignment and leadership; (2) policies and processes; (3) human capital; and (4) information management and stewardship. Assessments conducted using this Acquisition Framework can continue to be leveraged in meeting the requirements of the current update to OMB Circular No. A-123.

These guidelines are based on GAO's Framework for Assessing the Acquisition Function at Federal Agencies ([GAO-05-218G](#)) and can continue to be leveraged in meeting the requirements of the current update to OMB Circular No. A-123. Each of the elements of OMB's Acquisition Framework is reviewed below in relation to the [Green Book](#). The critical factors contained in each element of the acquisition framework are used where possible to depict these similarities and differences. The following illustrative table is included in setting out concepts that are common to both OMB's acquisition framework and the [Green Book](#) and required by the [Green Book](#), but not part of the acquisition framework.

---

<sup>21</sup> Traditionally, the Risk Management Framework was a framework to help agencies address information security and related risks in the authorization process for Federal information systems. NIST has published a suite of standards and guidelines that describe how to implement an agency-wide risk management framework. As of the date of this publication, many of the existing NIST standards and guidelines that detail how to implement an agency-wide risk management framework do not fully address the role of privacy and agencies' privacy programs. In the future, NIST may revise or develop standards and guidelines to further clarify how privacy and agencies' privacy programs are integrated into the Risk Management Framework.

**Table 7 Comparison of OMB Acquisition Framework and GAO Green Book**

Common to Both	Differences Required by the Green Book
<ul style="list-style-type: none"> <li>Aligning Acquisition with Agency Mission and Needs</li> <li>Commitment from Leadership</li> </ul>	None
<ul style="list-style-type: none"> <li>Planning Strategically</li> <li>Effectively Managing the Acquisition Process</li> <li>Promoting Successful Outcomes of Major Projects</li> </ul>	Management Responsibility for considering Fraud Risks
<ul style="list-style-type: none"> <li>Valuing and Investing in the Acquisition Workforce</li> <li>Strategic Human Capital Planning</li> <li>Acquiring, Developing, and Retaining Talent</li> <li>Creating Results-Oriented Organizational Cultures</li> </ul>	Management Responsibility for considering Fraud Risks
<ul style="list-style-type: none"> <li>Identify Data and Technology that Support Acquisition Management Decisions</li> <li>Safeguarding the Integrity of Operations and Data</li> </ul>	None

Agencies should continue their prior assessment activities under the acquisition framework to comply with the 2014 revision of the [Green Book](#). For example, the framework describes the Commitment from Leadership element to include management providing clear, strong and ethical executive leadership, and effective communication, and continuous improvement. These activities align with the [Green Book](#) principles that require an entity to demonstrate commitment to integrity and ethical values, while ensuring that management should communicate the necessary quality information both internally and externally.

One required [Green Book](#) principle that is absent from the current acquisition framework is management’s consideration for potential fraud when identifying, analyzing and responding to risks. Agencies must consider fraud risks in their strategic plans, and ensure agency professionals involved in planning for, reviewing, awarding, and managing deliverables under contract and throughout the acquisition lifecycle receive training on fraud indicators and risks. Additional guidance covering administrative actions and procedures for preventing fraud in emergency responses and contingency operations can be found in OMB’s emergency acquisitions guide<sup>22</sup> and in the Federal Acquisition Regulation (FAR).

### **C. Managing Grants Risks in Federal Programs**

On December 26, 2013, OMB published the final guidance, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (“Uniform Guidance”) 2 CFR 200. These new requirements set forth standards for obtaining consistency and uniformity among Federal agencies for the audit of non-Federal entities expending Federal awards. The requirements seek to effectively focus Federal resources, improve Federal grant

---

<sup>22</sup> Memorandum for Chief Acquisition Officers Senior Procurement Executives. Emergency Acquisitions Guide 1/14/2011. <http://www.whitehouse.gov/omb/procurement>



award performance, and create a government-wide framework for ensuring effective fiscal management of Federal grants. In addition, the requirements in 2 CFR 200.501, Audit Requirements, reduce the administrative burden on recipients by increasing the single audit threshold to \$750,000 in Federal award expenditures per year. The guidance in 2 CFR 200.205 requires Federal awarding agency review of risk(s) posed by applicants, risk evaluation(s) whenever making new awards, and authorized use of a risk based approach.

Within each Federal Agency, there is a shared interest for management and oversight of Federal grant dollars from both a financial management and grants management perspective. Leveraging the risk-based perspective, the internal controls framework should serve as a mechanism to ensure effective and efficient allocation and use of Federal grant dollars. Agencies must consider fraud risks in their strategic plans and ensure Federal officials involved in planning for, awarding, and managing grants and other forms of financial assistance receive training of fraud indicators and risk.

In addition, the Federal Government has a number of complex inter-dependencies with State and local governments, and other recipients of Federal funding. From an ERM perspective, these inter-dependencies are called the “extended enterprise” impacts the Agency’s risk management, and give rise to certain additional risks, which need to be considered in the Agency’s risk profile. Finally, ERM and use of data analytics is an emerging best practice; examples include:

- **Pre-award Decision Support:** Appropriate tools and data analytics made available to Federal awarding agencies to properly conduct risk analysis.
- **Pre/Post Award Monitoring Plans and Activities:** Federal awarding agencies use of relevant data to determine risks and take appropriate action prior to making awards.
- **Award Grantee Risk Mitigation:** Federal awarding agencies plan for and execute monitoring and mitigation activities meeting their specific needs.
- **Grant Policy Monitoring Standards:** Federal awarding agencies manage grant portfolios using a common set of risk-based standards.

#### **D. Managing Antideficiency Act Risks**

The Antideficiency Act (ADA) imposes restrictions on the amounts of obligations or expenditures that agencies may make. ADA violations are ultimately reported to the President, Congress, and the Government Accountability Office. An ADA violation may be a symptom of an underlying control deficiency. OMB Circular No. A-11, Section 150, Administrative Control of Funds outlines requirements for the administrative control of funds under the ADA. Section 150.3 explains the relationship between an agency’s internal controls and its fund controls. In addition, OMB Circular No. A-11, Section 145, Requirements for Reporting Antideficiency Act

Violations, provides more information about the ADA, and also provides agencies with guidelines for reporting violations. The Agency's risk profile as described in Section II must include a review of the agency's budget authority, from sources such as appropriations legislation, and identify any areas in which there is a risk of violating the ADA.

TAB B

RISK ASSUMED II

APPENDIX C

OMB Circular No. A-11, Section 230,  
Agency Strategic Planning (A-11)

FEBRUARY 2018

## SECTION 230—AGENCY STRATEGIC PLANNING

**Table of Contents**

- 230.1 What is an agency Strategic Plan?
- 230.2 What is the purpose of strategic planning?
- 230.3 What content is included in the agency Strategic Plan?
- 230.4 What timeframes must be established for achieving strategic goals and objectives?
- 230.5 When must agencies next update their Strategic Plan according to the GPRA Modernization Act and what is the timeline for Strategic Plan development?
- 230.6 What is an effective strategic goal?
- 230.7 What is an effective strategic objective?
- 230.8 Must the agency's strategic objectives be comprehensive, reflecting the major mission activities that the agency undertakes?
- 230.9 Are agencies required to set management-focused objectives addressing management functions such as financial management, acquisition, human capital, information technology, etc.?
- 230.10 What is an effective management objective?
- 230.11 Are agencies required to address the agency specific contributions to Cross-Agency Priority Goals (CAP) within the strategic plan?
- 230.12 Who should prepare the agency strategic goals and objectives?
- 230.13 What is the timeline for agencies to obtain input from OMB on the Strategic Plan?
- 230.14 What must be provided to OMB in the strategic plan draft?
- 230.15 What input should agencies solicit outside the Executive Branch in the development of Strategic Plans and when?
- 230.16 Can an agency consult with other agencies within the Executive Branch in the development of Strategic Plans?
- 230.17 How should agencies publish Strategic Plans and deliver them to Congress?
- 230.18 Can Strategic Plans be updated in the interim, before the end of the four-year revision cycle?
- 230.19 How should interim updates be communicated or published?

**Summary of Changes**

Describes Strategic Plan content and timeframes for development with the FY 2019 Budget as required by GPRA Modernization Act 2010.

Updates guidance to encourage interagency coordination in the development of Strategic Plans in instances where multiples agencies have shared strategic goals and objectives.

**230.1 What is an agency Strategic Plan?**

The GPRA Modernization Act 2010 aligns strategic planning with the beginning of each new term of an Administration, requiring every Federal agency to produce a new Strategic Plan by the first Monday in February following the year in which the term of the President commences. The Strategic Plan, therefore, presents the long-term objectives an agency hopes to accomplish at the beginning of each new term of an Administration by describing general and long-term goals the agency aims to achieve, what actions the agency will take to realize those goals, and how the agency will deal with challenges and risks that may hinder achieving results.

The Strategic Plan will define the agency mission, long-term goals, strategies planned, and the approaches it will use to monitor its progress in addressing specific national problems, needs, challenges, and opportunities related to its mission. It explains the importance of the goals, appraises the agency's capabilities, assesses the operating environment and provides for evaluations and other studies to inform agency actions. The Strategic Plan should explain why goals and strategies were chosen, discussing the relevant evidence supporting the selected goals and strategies. Because many agency missions, programs and strategies are statutory in nature, some of the strategic plan is expected to be more descriptive of those past decisions, whereas other parts of the strategic plan should reflect important strategic decisions in response to a recent agency analysis of the operating environment, Administration priorities or other emerging factors, for example.

An agency's Strategic Plan should provide the context for decisions about performance goals, priorities, strategic human capital planning and budget planning. It should provide the framework for the detail published in agency Annual Performance Plans, Annual Performance Reports and on Performance.gov. Agencies need to translate the long-term goals in their Strategic Plans to strategic objectives and then to performance goals, including Agency Priority Goals, in the Annual Performance Plan.

Because the Strategic Plan focuses on long-term objectives, it is important that agencies consider risks and how risks change over time during formulation of the plan. Considering risk management in early stages of the strategic planning process will ensure that the agency's management of risk is appropriately aligned with the organization's overall mission, objectives and priorities. (See more on enterprise risk management in section [270](#) and performance planning in section [240](#)). Incorporating strategic foresight into the strategic planning and review process is one method for facilitating the achievement of long-term goals. Strategic foresight is a method for systematically considering a longer time horizon and broader scope of issues than other forms of planning. Integrating strategic foresight in the planning process also facilitates a systems approach to problem solving and may help an agency better prepare for future threats or take early advantage of emerging opportunities. The systems approach of strategic foresight also encourages organizational communication to avoid the "silo effect," in which problems are viewed in isolation. Foresight methodologies may vary by agency depending on its mission and operating environment, but examples of strategic foresight methodologies include scanning, trend analysis, and scenario planning. Opportunities for cross-agency foresight coordination are also encouraged to be explored where appropriate.

## 230.2 What is the purpose of strategic planning?

In addition to fulfilling the GPRA Modernization Act requirements, strategic planning serves a number of important management functions related to achieving an agency's mission. Strategic planning is a valuable tool for communicating to agency managers, employees, delivery partners, suppliers, Congress, and the public a vision for the future. An agency's strategic goals and objectives should be used to align resources and guide decision-making to accomplish priorities to improve outcomes. It should inform agency decision-making about the need for major new acquisitions, information technology, strategic human capital planning, evaluations, and other evidence-building and evidence-capacity building investments. Strategic Plans can also help agencies invite ideas and stimulate innovation to advance agency goals. The Strategic Plan should support planning across organizational operating units and describe how agency components are working toward common results. An agency formulates its Strategic Plan with input from Congress, OMB, the public and the agency's personnel, partners, and stakeholders and makes the plan easily accessible to all. The agency's process for establishing and managing strategic goals and objectives should fulfill these important roles:

**Leadership.** The strategic goals and objectives communicate the Administration's priorities and direction through a unified vision, long-term goals, and supporting strategies. The Strategic Plan features strategic goals and objectives that state what the agency wants to accomplish in terms of outcomes or results.

**Planning.** The Strategic Plan is the foundation of an agency's planning system because it provides direction for all programmatic and management functions used to execute the strategies needed to reach goals.

Executives should use the Strategic Plan to provide guidance to agency components for planning their program implementation, including the alignment of information technologies and human capital resources to support improved outcomes and cost-effectiveness. The Strategic Plan should not, however, be a binding document that prevents agencies from learning from experiences and adapting their plans to changing circumstances. Instead, the strategic goals and objectives should be updated over time, incorporating agency learning, and emergent or external factors that may impact agency implementation.

**Management.** After the planning process, the agency uses the strategic goals and objectives to guide implementation and management. Each strategic goal should be supported by a suite of strategic objectives and performance goals. These, in turn, should be supported by other indicators used to monitor and interpret progress. The annual performance planning, human capital planning and budget processes jointly support the agency's implementation of the strategic goals and objectives by establishing resource allocations, refined strategies, activities, indicators, targets, and milestones in more detail. Agency Strategic Plans provide the framework for other plans and reports where agency performance goals and related analyses are communicated and monitored and revised when needed. For more information on management toward the strategic goals and objectives, see section [270](#) regarding the strategic review which includes information on the link between strategic planning and enterprise risk management.

**Engagement.** The strategic goals and objectives in an agency Strategic Plan are a tool to engage external entities to enlist their ideas, expertise, and assistance, including Congress, the public and the agency's stakeholders. For example, because delivery partners external to the Federal Government can be critical in accomplishing agency objectives, agencies may want to engage them in identifying potential goals and strategies to accelerate progress.

### **230.3 What content is included in the agency Strategic Plan?**

Agencies should plan to address the content as established in section [210](#) for the February 2018 publication of the new agency Strategic Plan and should use strategic reviews to help the agency identify the most effective long-term strategies.

### **230.4 What timeframes must be established for achieving strategic goals and objectives?**

The strategic goals and objectives should be established for a period of not less than four years forward from the fiscal year in which it is published, starting the first Monday in February of any year following the year in which the term of the President commences. Agencies may set strategic goals for longer periods of time. See section [230.17](#) regarding interim updates.

Strategic Plan:

- Publication February 2018 covers FYs 2018-2022
- Publication February 2022 covers FYs 2022-2026

The draft strategic goals and objectives should inform strategic human capital planning (consistent with 5 CFR Part 250) and agency budget submission to OMB in September 2017, which will include the FY 2019 draft APP. Detailed performance information supporting the strategic goals and objectives, such as draft performance goals, and indicators, are required to be provided in the APP draft submitted to OMB in September 2017, accompanying the agency's FY 2019 budget request. Agencies that do not submit a budget to OMB in September should still submit the draft APP to OMB for review.

### **230.5 When must agencies next update their Strategic Plan according to the GPRA Modernization Act and what is the timeline for Strategic Plan development?**

Agencies are required to publish an updated Strategic Plan, which meets requirements of the GPRA Modernization Act, concurrent with the publication of the FY 2019 President's Budget in February 2018.

After the February 2018 publication, agencies must issue a new Strategic Plan in February 2022. Agencies should prepare the new Strategic Plan by applying information learned from strategic reviews as they are conducted.

Agencies should prepare the Strategic Plan initial draft by June 2, 2017 in order to inform the development of the FY 2019 budget submission and FY 2019 Annual Performance Plan, which will also include FY 2018-2019 Agency Priority Goals. Continued refinements to the initial draft Strategic Plan will be expected prior to publication in February 2018. Agencies may work with OMB to make adjustments to the Strategic Plan draft submission if needed.

### **230.6 What is an effective strategic goal?**

Strategic goals should reflect the broad, long-term, outcomes the agency aspires to achieve by implementing its mission. Strategic goals communicate the agency efforts to address national problems, needs, challenges, and opportunities on behalf of the American people. Both the way strategic goals are framed and the substance they communicate are important to consider. Strategic goals should reflect the statutory mission of the agency, and most agency activity will align to the strategic goals. Strategic goals need not be as specific as strategic objectives, however, and need not reflect every activity that the agency must undertake to accomplish its mission.

Stylistically, strategic goals should be simple statements which are neither long nor overly complex. Some guidelines for developing these include:

- Use language that the public will understand and avoid highly technical terms that are very specific to technical or professional fields.
- Use language that expresses future direction or vision, and include active or directional verbs such as strengthen, support, maintain, improve, reduce, etc.
- Be specific enough for the public to clearly understand how the goal supports the agency's mission and communicates the agency's unique responsibilities.

For example, strategic goals such as "Improve Safety" do not communicate the agency's specific efforts in this outcome area. Better specificity might be "Maintain and Improve the Safety of America's Transportation" for the Department of Transportation. If desired, short headers may be used preceding the strategic goal statement (e.g. Safety: Maintain Safe and Healthy Workplaces), and a separate field will be provided in Performance.gov for the 'header' in addition to the full strategic goal statement.

Additional examples of strategic goals are:

- Strengthen Access and Quality of Healthcare for the American People
- Increase Children's Access to Safe, Nutritious, and Balanced Meals
- Strengthen the Nation's Housing Market To Bolster the Economy and Protect Consumers

### **230.7 What is an effective strategic objective?**

Strategic objectives reflect the outcome or management impact the agency is trying to achieve and generally include the agency's role. They express more specifically the results or direction the agency will work to achieve in order to make progress on its mission. Although objectives are usually outcome-oriented some objectives may be established to communicate the breadth of agency efforts – such as management objectives or crosscutting objectives that support multiple strategic goals. For the purpose of display on Performance.gov, strategic objectives may be described as:

- **Mission Focused.** A type of strategic objective that expresses more specifically the path an agency plans to follow to achieve or make progress on a strategic goal.
- **Mission Focused (Crosscutting/Other).** A type of strategic objective that is not directly tied to a single strategic goal, but may be tied to several or none. In some circumstances agencies perform statutory or crosscutting activities which are not closely tied to a single strategic goal.
- **Management Focused.** A type of strategic objective that communicates improvement priorities for management functions such as strategic human capital management, information technology, or financial stewardship. This may also be referred to as “Management Objective.”

Agencies should treat strategic objectives, (including mission, management, crosscutting, or other) as a primary unit for strategic analysis and decision-making. It is important to develop strategic objectives that enable a review of progress both on effectiveness of implementation and the impact made on ultimate outcomes, using a variety of sources of evidence. When developing each objective, the agency should consider how to measure progress toward achieving it, such as considering which performance indicators and other sources of evidence are most useful to understand progress and assess if current strategies are effective.

The following guidelines should be considered in crafting mission-focused strategic objectives:

- **Purpose: Will the strategic objective align agency efforts to achieve a desired outcome, and facilitate improved decision-making?** The purpose of each strategic objective is to align agency efforts toward achieving the intended outcome. Objectives should be meaningful and inspiring to agency leadership, program managers, and front-line employees, and their ongoing implementation should stimulate analysis and decisions which lead to improved outcomes. Strategic objectives should be defined to facilitate decision-making at the agency, as well as decision-making by the agency’s stakeholders. It should be possible to identify the lead office and other responsible offices for each strategic objective, and to identify the programs, activities and strategies utilized to achieve the objective. In some cases, objectives may be chosen which cut across organizational or programmatic silos in order to facilitate cross-organization management to improve outcomes or realize a better return on investment.
- **Assessment: Can progress on the strategic objective be reasonably assessed?** Agencies are required to annually assess progress toward achieving the intended outcomes of each strategic objective, as part of the strategic review (See section [270](#)). Considerations when determining if a strategic objective will support a meaningful assessment include:
  - Strategic objectives should be articulated so they express future direction or vision, and include active or directional verbs such as strengthen, support, maintain, improve, reduce, etc. The objective should be framed so it can serve as a standard against which an assessment can reasonably be performed (i.e., it is reasonable to say if progress had been made toward the objective and whether or not the objective was met).
  - Each strategic objective should have some means of assessing progress both on effectiveness of implementation and progress toward ultimate outcomes (e.g., performance indicators that can be analyzed to assess likely impact of agency action, evaluations).
  - An objective which includes a diverse set of outcomes will be more difficult to assess than objectives expressing a single outcome or multiple closely related outcomes.
  - The more ambiguity there is in the strategic objective statement as to the intended outcomes, the more challenging it will be to conduct a meaningful assessment.



- **Scope: Is the scope of the objective appropriate?** Strategic objectives should break down the broader, mission-oriented strategic goals to a level that reflects the impact or outcome the agency is trying to achieve through its programs. In general, strategic objectives will not be quantitative, but will add more specificity to the strategic goals and act as a bridge between the agency's strategic goals and more specific quantitative or alternative form performance goals.

The full set of an agency's strategic objectives will not necessarily capture the full depth and detail of agency activities. Many agency activities will be described through narrative supporting a strategic objective, or through the establishment of performance goals at a more granular level of agency planning, rather than through inclusion in the strategic objective statement. In general, agencies should have approximately 2-10 strategic objectives for each strategic goal; however the number may vary by agency and mission areas.

- **Clarity: Is it understandable?** Strategic objectives should be relatively simple statements that clearly communicate the outcome or impact that is desired. Statements should not be too long or complex since there will be strategies and other narrative supporting each. Agencies should use language that the public will understand and should avoid jargon.
- **Uniqueness: Is the objective defined in a way that clarifies the agency's role and mission?** In some cases, it may be difficult to understand the objective unless the agency's role is communicated. In these cases, the strategic objective should differentiate the agency's efforts from other agencies in a particular outcome area. For example, many agencies may be working to impact economic development; however, each organization may be responsible for a different facet, using different programs, interventions and strategies (e.g., housing rehabilitation vs. small business assistance). To the extent these distinctions can be made within the strategic objective statement, agencies should do so by clarifying the agency role or communicating the desired program results in summary. Alternatively, the strategies and other narratives that describe what the agency will do to execute on the strategic objective should be used to help to clarify the agency role.

Examples of mission-focused strategic objectives:

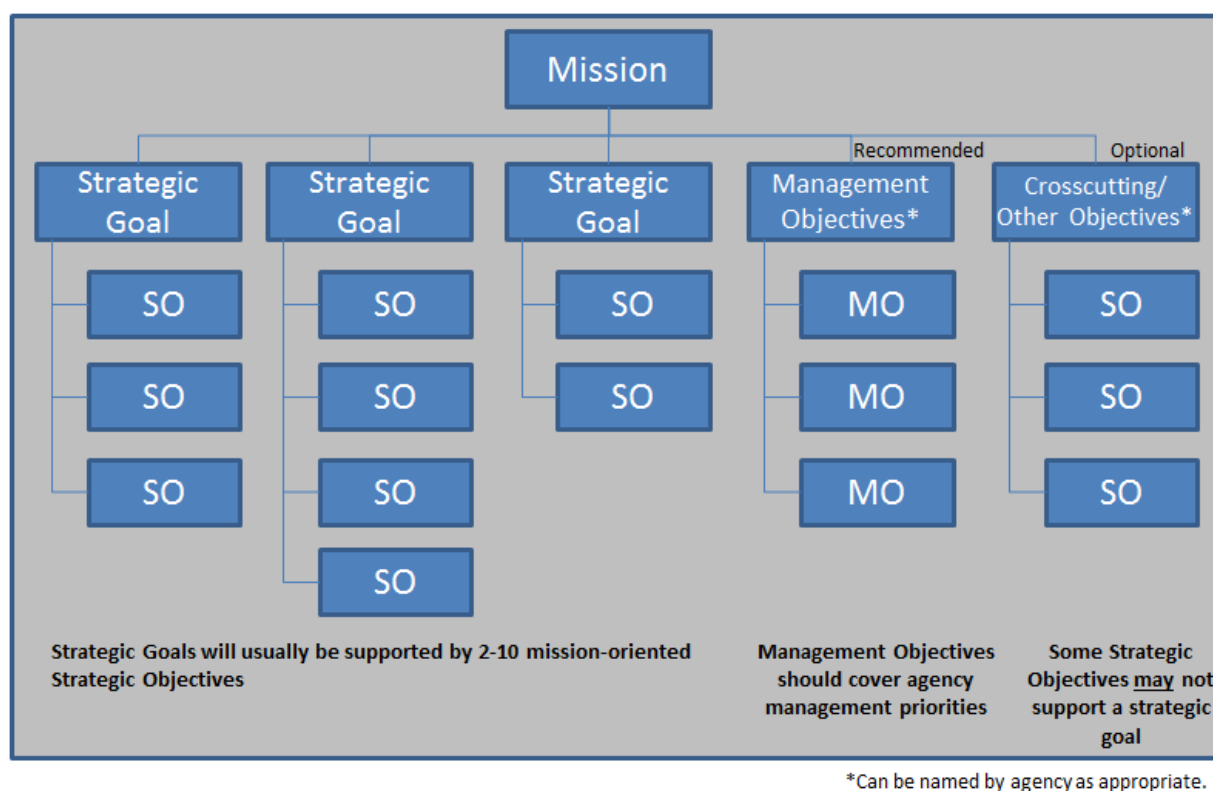
- Expand international markets for U.S. firms and inventors by improving the protection and enforcement of intellectual property rights
- Improve intellectual property protection by reducing patent pendency, maintaining trademark pendency, and increasing the quality of issued patents and trademarks
- Enhance national preparedness through a whole community approach to emergency management
- Prosecute those involved in terrorist attacks
- Improve public financial management and strengthen financial systems of developing countries by providing assistance through USAID programs.
- Substantially reduce the number of families and individuals with severe housing needs by expanding access to housing assistance
- Protect and restore watersheds and aquatic ecosystems
- Advance earth system science to meet the challenges of climate and environmental change

**230.8 Must the agency’s strategic objectives be comprehensive, reflecting the major mission activities that the agency undertakes?**

Yes. The strategic objectives should generally encompass the agency’s mission and scope of responsibilities, including statutory responsibilities. However, encompassing the *scope* of mission activities does not mean that the strategic objectives will cover the *depth and detail* of agency activities. There will be many cases where agency activities are too detailed to be included in the strategic objective statement or associated description, but are relevant to support an objective or multiple objectives. In some cases, these activities will be included in supporting narrative in the Annual Performance Plan.

The graphic below shows the relationship between Strategic Goals and Strategic Objectives, including management-focused and crosscutting objectives.

Example illustration of goal and objective relationships:



**230.9 Are agencies required to set management-focused objectives addressing management functions such as financial management, acquisition, human capital, information technology, etc.?**

OMB encourages agencies to establish management-focused objectives that reflect key priorities of the agency, such as a significant effort to improve performance across the organization. Agency leadership may opt to include a management objective or objectives that reflect these significant agency-specific priorities. In Performance.gov, management objectives will be listed under a separate category, similar to the categorization of strategic objectives under strategic goals. Each kind of strategic objective has the same management and public reporting requirements.

**230.10 What is an effective management objective?**

Management objectives communicate improvement priorities for management functions such as strategic human capital management, information technology, sustainability or financial stewardship. In general, these efforts will cut across the organization and should reflect priorities that leadership would like to emphasize over the period of performance established in the strategic plan. These key management efforts need not reflect all the important operations or management functions of the agency (e.g.; budget or legal functions) rather they should reflect broad, strategic-level decisions of emphasis or describe a relatively significant performance improvement change that affects most of the organization.

Management and operation functions not reflected in the strategic plan as management objectives should be addressed among performance goals in the Annual Performance Plan or in agency operational plans. Strategies supporting mission-oriented strategic objectives or strategies in the Annual Performance Plan should identify key operational processes, human capital, training, skills, technology, information and other management resources where they are relevant to the implementation of mission-focused strategic objectives.

Examples of management objective:

- *Financial Management:* Fight fraud and work to eliminate improper payments through increased emphasis on agency program integrity initiatives.
- *Strategic Human Capital Management:* Invest in the agency's employee recruitment, hiring, training, work-life programs and performance management so staff is engaged to more effectively serve small businesses.

**230.11 Are agencies required to address the agency specific contributions to Cross-Agency Priority Goals (CAP) within the strategic plan?**

Yes. See sections [210](#) and [220](#) for details.

**230.12 Who should prepare the agency strategic goals and objectives?**

The development of strategic goals and objectives is an inherently governmental function, and the plan is to be drafted only by Federal employees. Agencies should engage their organizational components (employees), Congress, OMB, delivery partners and other stakeholders in the development of the strategic goals and objectives.

When preparing the plan for publication, agencies may be assisted by non-Federal parties, such as consultants or contractors who are hired specifically to provide technical input on the design and assembly of the plan, and who are not solicited for their input on policy or budget issues. The Strategic Plan should include an acknowledgment and brief description of the contribution by a non-Federal entity in preparing the plan, if applicable.

**230.13 What is the timeline for agencies to obtain input from OMB on the Strategic Plan?**

Agencies should provide the initial draft Strategic Plan to OMB no later than June 2, 2017, using the content described in section [210](#) and leveraging findings derived from annual strategic reviews and the initial risk profile (see [OMB Circular A-123](#)) to develop the plan. The planned schedule provides four weeks for the initial OMB review and feedback starting in June 2017.

A full draft of the strategic plan and a draft annual performance plan will be provided no later than the FY 2019 budget submission in instances where an alternate Strategic Plan submission timeline was worked out in advance with OMB. After incorporating initial OMB comments and external stakeholder input, agencies

must provide the final draft Strategic Plan to OMB for clearance, no later than December 22, 2017, providing a minimum of two weeks for the final OMB clearance. The detailed timeline is summarized in the table below:

Date	Action
June 2, 2017	Agencies submit for OMB review initial draft Strategic Plan covering FYs 2018-2022. Specific components of initial draft Strategic Plan submissions include: -Agency Mission Statement -Draft Strategic Goals -Draft Strategic Objectives, including a short description of each -FY 2018-2019 Agency Priority Goal areas
June 30, 2017	Agencies will have received initial feedback from OMB by June 30.
September, 2017	Agencies submit for OMB review: -Full draft of FYs 2018-2022 Strategic Plan that incorporates the detailed content requirements provided in section <a href="#">210.11</a> -Draft full action plans for FY 2018-2019 Agency Priority Goals -Draft FY 2019 Annual Performance Plan
November, 2017	Agencies will have received feedback from OMB on full draft submission of FYs 2018-2022 Strategic Plan, FY 2018-2019 APGs, and FY 2019 Annual Performance Plan
December 22, 2017	Final draft Strategic Plan submitted to OMB for clearance
January, 2018	For final OMB clearance, agencies submit: -FY 2018-2019 APG full action plans and Q1 Quarterly Performance Update -FY 2019 Annual Performance Plan -FY 2017 Annual Performance Report
February, 2018	Concurrent with the FY 2019 President's Budget, publish: -FYs 2018-2022 Agency Strategic Plan -FY 2019 Annual Performance Plan -FY 2017 Annual Performance Report -FY 2018-2019 APG action plans and Q1 Quarterly Performance Update

#### 230.14 What must be provided to OMB in the strategic plan draft?

All agencies are encouraged to submit full draft Strategic Plans, using the content required by the table in section [210](#), by posting the draft document on MAX at <https://max.omb.gov/community/x/C5VxIQ>. For large agencies, the minimum requirements will also be collected through the PREP tool in Performance.gov for internal Government deliberation. Small agencies should submit the draft strategic plan via MAX at <https://max.omb.gov/community/x/C5VxIQ>.

At a minimum, the June submission to OMB via Performance.gov must include:

- The Agency's Mission Statement;
- Draft Strategic Goals;
- Draft Strategic Objectives, including a short description for each; and

- Draft FY 2018-2019 Agency Priority Goal areas

OMB will review the submissions, coordinate with other offices in the Executive Office of the President, as appropriate, and provide initial feedback to agencies within four weeks of the June submission. The draft strategic goals and objectives should inform the agency FY 2019 budget submission in September 2017, which will include the FY 2019 draft Annual Performance Plan. Detailed performance information supporting the strategic goals and objectives, such as FY 2018-2019 Agency Priority Goals, performance goals, and indicators, are required to be provided in the Annual Performance Plan draft submitted to OMB in September 2017. Agencies that do not submit a budget to OMB in September should still submit the draft Annual Performance Plan to OMB for review.

A full draft of the Strategic Plan and a draft Annual Performance Plan should be provided with the FY 2019 agency budget submission in September 2017, and be informed by the key findings of annual strategic reviews as well as the complete risk profile completed by agencies as part of the strategic reviews conducted in spring 2017. Agencies should submit the required portions through the PREP tool and should also post the full draft Strategic Plan on MAX at <https://max.omb.gov/community/x/C5VxIQ>.

### **230.15 What input should agencies solicit outside the Executive Branch in the development of Strategic Plans and when?**

When preparing a Strategic Plan, agencies must consult with the Congress and should consider both majority and minority views as well as the views of other interested and potentially-affected parties, including non-Federal stakeholders and delivery partners. These consultations generally should occur after the initial draft is reviewed by OMB, during the summer prior to publication, though agencies may determine alternative outreach approaches, such as ongoing agency communications and contact processes, in consultation with OMB. Agencies should work with their legislative affairs offices to determine the best ways to consult with Congress on the strategic plan, in advance of finalizing the plan with OMB.

Consultation with external stakeholders could include hosting public meetings on the draft plan or draft goals or posting the draft plan on the internet and inviting comment after OMB has been provided an initial draft. Agencies may consider using the existing published Strategic Plan to begin earlier consultations with Congress and other stakeholders before a more fully-developed revision is completed. This approach should allow stakeholders to engage early in the development process. Agencies must consult with Congress at least every two years on their Strategic Plans and should briefly note how feedback was integrated.

### **230.16 Can an agency consult with other agencies within the Executive Branch in the development of Strategic Plans?**

Yes. Agencies are encouraged to consult with other agencies within the Executive Branch in the development of Strategic Plans, as the outcomes of some strategic goals and objectives that an agency's strategic plan seeks to achieve may require interagency coordination of programs and resources. Interagency coordination in the development of the agency strategic plan will help ensure the appropriate alignment of resources in instances where agencies have shared strategic goals and objectives. Agencies that want assistance should contact OMB.

### **230.17 How should agencies publish Strategic Plans and deliver them to Congress?**

The GPRA Modernization Act of 2010 requires agencies to make the Strategic Plan available on a central website in machine readable format, and notify the President and Congress of its availability (See section [210](#) on Performance.gov.).

Agencies that were not required to establish Agency Priority Goals on Performance.gov, will publish Strategic Plans on the agency's website, and will provide a hyperlink for publication on Performance.gov that directs readers to the agency plan on the agency's website.

Agencies will notify the OMB Director of the agency's final Strategic Plan by approving the content on Performance.gov, and by providing the plan link to OMB at [performance@omb.eop.gov](mailto:performance@omb.eop.gov) if the content was not provided in Performance.gov. Related submissions or questions may be emailed to the same address.

Notification to Congress of the availability of the Strategic Plan on Performance.gov (or the agency website, if applicable) is transmitted electronically by the agency head. Transmittal emails are addressed to the Speaker of the House of Representatives, the President of the Senate, and the President pro tempore of the Senate.

#### **230.18 Can Strategic Plans be updated in the interim, before the end of the four-year revision cycle?**

Yes. Agencies may make adjustments to their Strategic Plan in advance of the four-year revision cycle prescribed by GPRA Modernization Act, as strategic reviews or external factors may impact changes to long-term decisions. In order to ensure the strategic goals and objectives reflect agency efforts throughout the Administration, agencies are encouraged to consider changes to their strategic goals and objectives as part of the strategic reviews. Revisions may occur based on results of strategic reviews, information gained through evaluations, external events, changes in legislation, changes in strategy, or other factors. While these changes will be encouraged to be made as part of the agency strategic review process, interim adjustments will also be considered throughout the year in response to major events. Interim adjustments do not alter the four-year revision cycle for Strategic Plans.

An agency does not need to consult with Congress or conduct outreach to potentially interested or affected parties when preparing interim adjustments, unless such adjustments reflect significant changes. Significant changes to an agency's Strategic Plan should be made using a more extensive update process with review by OMB. Congressional consultation requirements apply in these instances of significant change. In general, any updates to the agency strategic goals and strategic objectives should be made during the annual update of the Annual Performance Plan, concurrent with the release of the President's Budget in February.

#### **230.19 How should interim updates be communicated or published?**

Interim adjustments to the Strategic Plan, such as but not limited to new Agency Priority Goals, generally will not require a new publication of the full Strategic Plan. For example, an agency may append an interim adjustment (e.g., newly defined Priority Goals) to its budget submission or include the changes as a part of the Annual Performance Plan to OMB to address the needed adjustments to the Strategic Plan if any. Such interim adjustments should be published in the Annual Performance Plan that is sent to OMB in September and to Congress in February and should be made easily accessible to the public.

TAB B

RISK ASSUMED II

APPENDIX D

Federal Highway Administration  
Risk Management Process  
User Manual - 2013

FEBRUARY 2018



U.S. Department  
of Transportation  
**Federal Highway  
Administration**

# **Federal Highway Administration**

## **Risk Management Process**

### **User Manual**

**January 2013**



This page was intentionally left blank.

**RISK MANAGEMENT PROCESS USER MANUAL CONTENTS**  
How to update, revise, or put together your risk management plan  
*(Revised January 25, 2013)*

Background.....	1
Step 1 - Communication And Consultation .....	2
Step 2 – Identify Risk Context.....	3
Step 3 – Identify The Risks .....	4
Step 4 – Analyze the Risks .....	5
Step 5 – Prioritize The Risks.....	6
Step 6 – Identify and Prioritize Risk Responses .....	7
Step 7 – Monitor, Evaluate, and Adjust (The Risk Tracker) .....	8
Appendix A - Risk Management Process – Overview, Questions, Tools, Outputs .....	9
Appendix B - Impact Criteria Matrix .....	10
Appendix C - Likelihood Criteria Matrix.....	11
Appendix D - Heat Map.....	12
Appendix E – Glossary .....	13

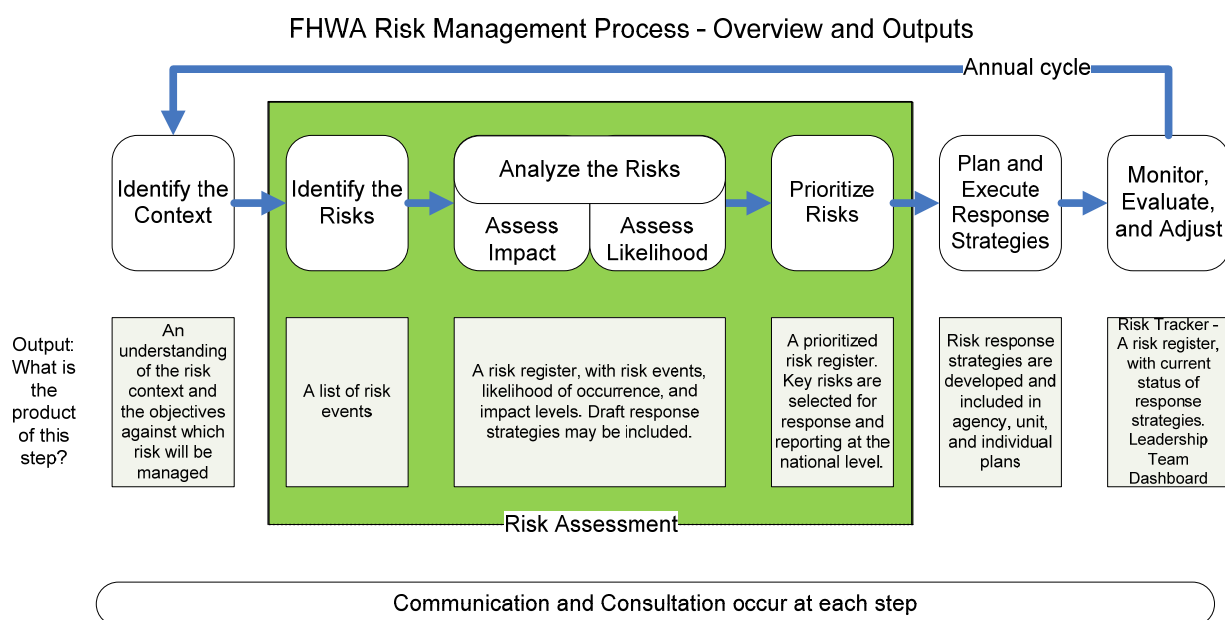
## BACKGROUND

This user manual gives brief instruction and explanation on the FHWA risk management process. Risk management is a tool for focusing limited resources to efficiently manage our programs and advance our strategic objectives. The goal of risk management within FHWA is to provide reasonable assurance that we understand the risks associated with achieving our agency's objectives and that we are responding appropriately.

The international definition of risk is “*the effect of uncertainty on objectives.*” By identifying risk events, their likelihood of occurrence and the impact they would have, FHWA can assess and prioritize those impacts and likelihoods; and determine and prioritize strategies to respond to them.

The objective of FHWA's risk management process is to establish a consistent approach to identify and prioritize program area risk events. Applying the principles of risk makes it possible to identify threats and opportunities; assess and prioritize those threats and opportunities; and determine and prioritize strategies so that we can decide how to address future issues affecting the Federal-aid and Federal Lands Highway Programs and national objectives. In FHWA, risk management is a way to:

- **Focus limited resources** – focus staff and budget resources to maximize opportunities and minimize events that threaten FHWA programs and national objectives.
- **Strengthen the ability to efficiently manage program delivery** – make informed decisions about the scope, approach, and intensity of our efforts.
- **Improve communication and manage risk corporately** – communicate consistently to leadership about what the Agency should focus on and why.



# STEP 1 - COMMUNICATION AND CONSULTATION

## *IN THIS STEP*

Communicate and consult with stakeholders as needed throughout the risk management process and cycle.

## *KEY QUESTIONS*

Who needs to be involved? How will we communicate and consult with them?

## *HOW TO DO IT*

Identify your stakeholders. Ask who can affect, be affected by, or perceive themselves to be affected by a decision or activity. For FHWA, stakeholders can be organizational leaders, Congress, state departments of transportation, tribes, other federal agencies, regional or metropolitan planning organizations, other local public entities, environmental or civic groups, or individuals. Stakeholders can be internal or external to the organization. Consider the desired outputs of communication and consultation, and decide where in your risk process to engage stakeholders.

## *TOOLS AND TECHNIQUES*

Communication and consultation involves the activities below when used to identify context, and assess, respond or monitor risks. These activities may occur throughout the risk cycle:

- formal and informal meetings with internal and external stakeholders;
- verbal or written reports, surveys, or emails;
- teams that address specific risks, programs, or objectives;
- leadership activities

Use your stewardship agreement, program areas, program assessments, strategic implementation plan and unit performance plans to consider who can affect, be affected by, or perceive themselves to be affected by a decision or activity regarding a specific program area or objective.

For assessable units, use the FHWA Federal Managers Financial Integrity Act (FMFIA) Unit Risk Profile to identify and document stakeholders. Stakeholders are identified and documented in the sections on organizational structure, management roles and responsibilities, operating and support locations, customers, business processes owners (under major business activities), and service level agreements.

## *EXPECTED OUTCOME*

It is expected that continuous communication and consultation throughout the risk assessment process will result in the identification of risks and response strategies that represent the perspective of both FHWA and key stakeholders. For a Federal-aid Division, it is expected that the process will involve the State Highway Administration and that the final determination of top risks and appropriate response strategies will be done in consultation with them.

## STEP 2 – IDENTIFY RISK CONTEXT

### IN THIS STEP

You will identify your objectives, gather information, understand the business environment, and determine how you will approach risk management. This is where you will think about unit, program, stewardship, oversight, or other objectives, consider your internal and external context, and establish the criteria for managing risk.

### KEY QUESTIONS

What are your objectives? What are the things to consider when we assess the risks of achieving our objectives? What criteria will we use to assess our risks? Who will do the assessment?

### *WHAT ARE YOUR OBJECTIVES?*

You will assess the risks involved in achieving your objectives. Your objectives may be influenced by the strategic implementation plan or by what you seek to achieve, including stewardship, at the program level or in some cases the project level.

### *WHAT INFORMATION DO I NEED (EXTERNAL CONTEXT)?*

Consider external environment in which the FHWA seeks to achieve its objectives. It includes but is not limited to the public, political, legal, regulatory, financial, technological, and economic; key drivers and trends having impact on the objectives of the organization; and relationships with, perceptions and values of external stakeholders. Use the FMFIA Unit Risk Profile to identify and document external context.

### *WHAT INFORMATION DO I NEED (INTERNAL CONTEXT)?*

The internal context is the internal environment in which the organization seeks to achieve its objectives. It is anything within the organization that can influence the way in which it will manage risk such as culture, structure and governance, goals and objectives, performance metrics, resources, internal stakeholders, information systems, decision making processes, policy, standards, and guidelines. A Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis can be helpful. Use the information in the FMFIA Unit Risk Profile to help identify and document internal context.

### *WHAT CRITERIA AND APPROACH WILL WE USE TO ASSESS OUR RISKS? (RISK MANAGEMENT CONTEXT)*

FHWA has adopted likelihood and impact as criteria to evaluate the significance of risk. These criteria should be used to assess the level at which risk requires a response and the level of that response. A unit's top 5-10 risks are considered top risks. Decide how you approach this process. You can use a multi-disciplinary team, rely on subject matter experts, or involve external or other internal stakeholders. Decide on the tools you will use to identify, assess and document your risks.

### EXPECTED OUTCOMES

At the end of this step you will have clarified the unit, program, stewardship, oversight, or other objectives for which you are assessing risk. You should have an understanding of the internal and external environment in which you are trying to achieve those objectives. You should know what approach you will use to identify risk, who will be involved, and what criteria you will use to assess risk.

## STEP 3 – IDENTIFY THE RISKS

### IN THIS STEP

You will generate a list of the barriers (threats) and enablers (opportunities) to achieving your objectives. Risk management is an art more than a science. This step is the art of turning threats and opportunities into risk statements. This is a way of verbalizing what it is you are making decisions about and why.

### KEY QUESTIONS

What events could happen that would affect my program areas or objectives? What are the corresponding impacts?

### DEFINITION

The international definition of risk is “*the effect of uncertainty on objectives.*” Risk events are the things that could happen sometime in the future that will trigger your threat or opportunity. A risk is a threat if the effect is a detriment to your ability to achieve an objective and a risk is an opportunity if it offers a benefit.

### HOW DO YOU IDENTIFY THE RISKS?

Generate a list of risks that answer the key questions. How you approach this process will affect the results and the time required to perform the analysis. A multi-disciplinary team provides a more complete perspective but requires time and facilitation. Relying on your subject matter expert may be quicker but doesn't always consider crosscutting threats and opportunities. Communication and consultation with State partners or other stakeholders provides mutual understanding and verification. State partners will likely need to play some role in mitigation of risk. If you have known risks from prior assessments, include them.

### THE RISK STATEMENTS

A simple narrative statement should be developed to describe each risk that is identified. The statement should give some context to the issue and describe the perceived impact from the risk. It may be helpful to use the “if/then” format to identify the risk events and the resultant impacts.

### EXPECTED OUTCOME

It is expected that this step will generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis. Identification should include risks whether or not their source is under the control of the organization. Risk identification should include consideration of the secondary and cumulative effects of particular impacts. It should also consider a wide range of impacts even if the risk source or cause may not be apparent. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what impacts can occur. All significant causes and consequences should be considered.

## STEP 4 – ANALYZE THE RISKS

### *IN THIS STEP*

You will assess your risks based on the impact of threat or opportunity being triggered and the likelihood of the event happening. Assessing your risks gives you a way to better understand and then prioritize them. Risk analysis involves consideration of the causes and sources of risk, their positive and negative impacts, and the likelihood that those impacts can occur.

As stated earlier risk assessment is more an “art” than a science. FHWA’s broad role in the implementation and oversight of the Federal-aid program lends to a qualitative risk assessment and therefore numerical risk levels are not encouraged in this guide.

### *KEY QUESTIONS*

What is the severity of this impact according to accepted agency criteria? What is the likelihood that this risk event will occur?

### *IMPACT ASSESSMENT*

The impact assessment is used to gauge how large the impact will be. Is there a threat to human life? Is there a threat to fraud waste and abuse? Is there an opportunity for technology implementation? Is there an opportunity to meet strategic goals?

Estimate the level of impact based on what will happen if the event occurs. Make the assessment based on data with a future projection or based on expert or a group’s knowledge and opinion of the risk being assessed. Use the risk impact criteria in the Appendix to inform your assessment and select an impact level of insignificant or neutral, minor, moderate, severe, or catastrophic for each risk.

### *LIKELIHOOD ASSESSMENT*

The likelihood assessment is used to gauge how likely an event is to occur. For example, events that may happen every day have a far higher likelihood than events that may only happen once in 10 years.

Estimate the likelihood based on data when available with a future projection OR based on an expert’s or a group’s knowledge and opinion of the risk being assessed. Certain conditions may increase or decrease the likelihood of a risk event and an impact. Use the risk likelihood criteria in the Appendix to inform your assessment and select a likelihood level of unlikely, possible, probable, or almost certain for each risk.

### *EXPECTED OUTCOME*

It is expected that step will provide a qualitative assessment of the likelihood of occurrence for each risk and the potential impact to objectives should that risk occur. FHWA has established impact and likelihood criteria to ensure some consistency within the agency for determining the risk levels.

## STEP 5 – PRIORITIZE THE RISKS

### *IN THIS STEP*

The purpose of this step is to examine the impact level and likelihood results from the analysis step to help determine a relative importance and a priority ranking for the risks. Creating a priority ranking communicates what are the most important issues on which you are making decisions. Not all of your priority risks will require actions. At this point it is recommended that you decide which risks represent your top risks without regard to resource constraints. Consideration of resources should be used to prioritize response strategies in the next step.

### *KEY QUESTIONS*

What are the impact level and likelihood of your risks? How do the risks compare, such as on heat-map? Which risks does leadership consider the “top risks?” Which risks will require a response?

### *TOOLS*

Sort your risks based on your likelihood and impact. A “heat-map” can be useful to for plotting risks based on the analysis results to visually compare risks. The heat-map is only a tool, and leadership must validate analysis results and the identification of top risks. Decide which represent your top risks and assign a priority to each.

### *LEADERSHIP VALIDATION*

Office leadership must validate the risk prioritization and identification of top risks. Leadership can provide a unit office perspective to normalize across objectives, programs and performance areas.

### *AT THE CORPORATE LEVEL*

Risks have relative importance within units based on local context. At a national level analysis may prove useful where context is similar, such among division offices or among HQ offices, but currently the top 5 to 10 risks for each unit are included in the agency Risk Tracker only to communicate risk information to leadership and to track implementation status for response strategies.

### *EXPECTED OUTCOME*

It is expected that this step will result in the prioritization of your identified risks as well as the identification of your 5-10 “top risks” that will be include in the corporate risk tracker. Prioritization and identification of top risks should be informed by the analysis results and validated by office leadership such that they represent the “unit” risks.



## STEP 6 – IDENTIFY AND PRIORITIZE RISK RESPONSES

### *IN THIS STEP*

You will decide what new strategies you may undertake, what existing strategies to continue, what business as usual strategies are acceptable, and if there are some strategies that make it possible to trim the level of effort required on programs with lower risk. Selecting the most appropriate risk response strategy involves balancing the costs and efforts of implementation against the benefits derived. Your risk response strategies will help you identify actions and priorities to be included in the office work plan and individual work plans

### *KEY QUESTIONS*

What actions will we take to mitigate, avoid, accept, transfer, or enhance our risks? What actions are important to take now? Are there ongoing actions to continue? Who is accountable, when will they start, and when will it be done?

### *DEFINITIONS*

Response strategies are the decisions we are making and actions we will take to deal with the risk.

- AVOID by not starting or discontinuing the activity that gives rise to the risk;
- ENHANCE in order to pursue an opportunity;
- MITIGATE by removing the risk or changing the impact / likelihood;
- TRANSFER by having another party take responsibility;
- ACCEPT by informed decision that your business as usual will be sufficient for dealing with a risk OR that if your risk does occur you will have a contingency plan for dealing with the consequences.

### *DOCUMENTING YOUR RISK RESPONSES*

Document which of the response strategies you will take, what you will do to implement the strategy, and when you will take the action. You may assign priorities to actions. You may carry over existing responses or identify multi-year actions or strategies to respond to a particular risk. Avoiding and Transferring may require little effort but document what you will do to make the avoidance and transfers happen. Mitigating and Enhancing strategies usually require activities such as technical assistance, training, strengthening partnerships, monitoring, tracking, or conducting a review. Are these actions that are or can be put in your unit plan or other plans?

### *EXPECTED OUTCOME*

It is expected that this step will result in strategies that respond to each of the known risks. Units should consider resource constraints to determine and prioritize appropriate response strategies. Where the unit will take action, the risk response strategies should include the action, a timeframe, and a responsible person or office. Response strategies may be included as activities in strategic, unit, project, or other plans.

## STEP 7 – MONITOR, EVALUATE, AND ADJUST (THE RISK TRACKER)

Progress in implementing risk response strategies provides a performance measure. The results can be incorporated into the organization's overall performance management, measurement and external and internal reporting activities.

### *IN THIS STEP*

In this step your “top risks” and the related response strategies are loaded into the Risk Tracker for agency-wide monitoring and tracking. Units should also have an approach for monitoring other known risks from year to year. This may be the risk tracker or a local risk register.. Follow up and measure the strategies you put in place. Did your strategies change your risk in terms of likelihood and/or impact?

### *KEY QUESTIONS*

What is the status of our response actions? Are they completed, in progress, not started, or has the action been deferred? Did the action have the desired effect? What is the residual risk and how should we respond?

### *USING THE RISK TRACKER*

The Risk Tracker is a central location for all units to load their top risks along with information regarding the implementation of response strategies. On a Quarterly basis the status of the response strategies are updated in the Risk Tracker and progress report to the leadership team. Have they been started, are they on schedule or completed, have they been deferred or cancelled?

### *AT THE CORPORATE LEVEL*

Seeing if events change likelihood or impact provides a general perspective. This helps communicate about changes in risks and successes in response strategies. The risk management process helps to communicate corporately about our programmatic decisions.

### *EVALUATE AND ADJUST*

On a yearly basis read through your risk statements. Do they need tweaking? Are there new risks in the program areas? If so edit and add. Reassess your likelihood and impact. Did the likelihood and impact value for each risk stay the same? If they changed as a result of actions your office has taken, use this as a performance indicator.

### *EXPECTED OUTCOMES*

It is expected that this step will result in a risk register, dashboard, or other report, to communicate the status of risk response activities. This includes whether an action has been started, completed, or delayed, and whether the action taken had the desired effect on the risk. It can also show what the residual risk is and where additional response is required. For FHWA assessable units, the Risk Tracker is used to communicate risks and their status.

## APPENDIX A - RISK MANAGEMENT PROCESS – OVERVIEW, QUESTIONS, TOOLS, OUTPUTS

Steps: What do I do?		Tools and Techniques: What are the questions and what tools can I use to answer them?	Output: What is the product of this step?
Communication and Consultation occur at each step	Who needs to be involved? How will we communicate and consult with them?	FMFIA Risk Profile, Stewardship Agreement	Meetings, verbal or written reports, surveys, teams, leadership activities
↓			
Identify the Context	What program or other objective areas will we assess? What are the things to consider when we assess them? What criteria will we use to assess our risks? Who will do the assessment?	FMFIA Risk Profile, Program Areas, Strategic Plan, SIP, Unit Plan	An understanding of the risk context and the objectives against which risk will be managed
↓			
Identify the Risks	What events could happen that would affect my program areas or objectives? What are the corresponding impacts? What are my If...then... statements?	Brainstorming Strengths, Weaknesses, Opportunities and Threats (SWOT) Subject matter experts Surveys	A list of risk statements
↓			
Analyze the Risks	What is the severity of this impact according to my criteria?	Impact Criteria	A risk register, with risk events, likelihood of occurrence, and impact levels. Draft response strategies may be included.
Assess Impact			
Assess Likelihood	What is the likelihood that this risk event will occur?	Likelihood Criteria	
↓			
Prioritize Risks	How do the risks compare? What is the relative ranking of each risk statement? Which risks does leadership consider the “key risks?” Which risks will require a response?	Heat Map Rank Order Risk Tolerance Leadership Validation Consultation	A prioritized risk register. Key risks are selected for response and reporting at the national level.
↓			
Plan and Execute Risk Response Strategies	What actions will we take to mitigate, avoid, accept, transfer, or enhance our risks? Are there ongoing actions to continue? What actions are important to take now? Who is accountable, when will they start, and when will it be done?	Response Context Corporate, Unit, and Individual Performance Plans	Risk response strategies are developed and included in agency, unit, and individual plans
↓			
Monitor, evaluate, and adjust	What is the status of our response actions? Are they completed, in progress, not started, or has the action been deferred? Did the action have the desired effect? What is the residual risk and how should we respond?	Risk Tracker Roll up, Dashboards, Monitoring, Response level	A risk register, with current status of response strategies. Risk Tracker - Leadership Team Dashboard

Impact Criteria Matrix

	Financial	Reputation	Business Operations	Legal and Compliance	Infrastructure Assets	Resources and Effort Required	Human and Natural Environment	Safety	Civil Rights	Economic
Catastrophic	Large unacceptable financial loss, severe budget variance. Critical long term impact on budget/finances, not recoverable within current or next fiscal year. Critical business functions could be vulnerable or ineligible. Systematic and extensive major fraud. Results in qualified audit opinion.	Very significant harm to image with substantial impact on effectiveness. Significant adverse community impact and condemnation. Consistent extreme negative media attention (months). Irreconcilable community loss of confidence in the organization's intentions and capabilities and possibly in the government. Secretary level intervention	Large and unacceptable operational impact, long term business interruption. System failure and overall survival of the organization is threatened. Full business disruption for more than one week or a key service more than two weeks. Majority of critical programs cannot be achieved. Secretary level intervention	Material compliance infraction. Significant prosecution and fines. Major litigation involving class actions. Major non-compliance with legislation.	Significant or critical infrastructure assets are destroyed. Significant or critical infrastructure assets are unusable for months.	Impact cannot be managed within the organization's existing resources and threatens the survival of the organization. Department Secretary level intervention.	The event will permanently affect the human and natural environment. The impact covers a wide area and is difficult to contain. The effects are irreversible. Threat to survival of flora, fauna, and or cultural heritage.	Many fatalities.	Program or critical component of a program declared unconstitutional the US Supreme Court, thereby effectively eliminating it nationally. Complete inability to achieve any of the program's objectives, or any objectives of a critical component of a program.	Significant, long lasting negative impacts to the economy of a major metropolitan area, a State or the nation
Major	Very significant financial loss, major budget variance. Significant impact on budget/finances/eligibility, not recoverable within current or next fiscal year. Significant fraud waste or abuse. Leads to material weakness.	Major embarrassment leading to significant impact on effectiveness. Considerable and prolonged community impact and dissatisfaction publicly expressed Community loss of confidence in the organization's and capabilities (weeks) Consistent negative media attention (weeks) Administrator or Executive Director level intervention	Unacceptable operational impact, short term business interruption. Continued capability of the organization is threatened. Full business disruption for up to one week or a key service up to two weeks. One or more critical programs, projects, or agency priorities cannot be achieved	Reportable compliance infraction. Major breach of regulations. Major litigation.	Non critical infrastructure assets are destroyed. Significant or critical infrastructure assets are unusable or restricted for weeks.	Impact requires significant long term management and organizational resources to respond.	Medium to long term impact to the the human and natural environment. The impact covers a wide area but can be contained. Able to be remediated but will require dedicated expert resources.	Fatalities or permanent disabilities.	Long-term impact on the protected rights, intended benefits, or ability to implement effective nondiscrimination programs. Numerous and continuous complaints in multiple program areas that cannot be addressed timely.	Significant economic disruption to a major metropolitan area or entire State
Moderate	Significant financial loss and variance to budget. Major impact on budget/finances/eligibility, may be recoverable within current year, but requires reprioritization. Limited instances fraud waste or abuse. Leads to several audit findings.	Moderate embarrassment impacting short term effectiveness. Community impact and concerns publicly expressed (days) Negative media attention (days) Loss of confidence by the community in organization processes Administrator or Executive Director level concern	Moderate operational impact, business not interrupted. Effectiveness and efficiency of major elements of the organization are reduced. Full business disruption for one day or a key service disruption up to one week. Ability to achieve one or more critical programs, projects, or agency priorities is reduced.	Significant compliance infraction. Serious incident requires investigation and legal representation to determine legal liability. Non compliance with regulation.	Some assets, not including significant or critical assets, are unusable or restricted for weeks.	Impact requires management and resources from a key area of the organization to respond.	Medium term impact to the the human and natural environment. Limited to a small area. Able to be remediated but will require intervention or management by external parties.	Injuries requiring medical treatment with possible fatalities.	Impact results in noncompliance affecting protected rights or intended benefits. Issues are addressed, but over unreasonably long period of time. Numerous complaints in one or more program areas.	Some economic disruption to a metropolitan area or portion of a State; impacts may or may not be long lasting
Minor	Minor financial loss, small budget variance. Slight but noticeable impact on budget/finances/eligibility, recoverable within year. Minor instances of fraud waste or abuse. Leads to audit findings.	Minor embarrassment, but no harm to image or reputation. Local community impact and concerns Occasional or once off negative media attention	Minor operational impact, business not interrupted. Effectiveness and efficiency elements of the organization are reduced, Partial business disruption for less than three days. Opportunity or ability to achieve objectives or deliver outcomes is affected.	Minor compliance infraction. Complex legal issue to be addressed.	A number of assets are unusable or restricted but can be replaced within an acceptable timeframe.	Impact requires additional local management effort and redirection of resources to respond.	Short term impact to the the human and natural environment. Able to be remediated through existing processes. Minimal threat to flora, fauna, and or cultural heritage	Injuries requiring medical treatment.	Minor impact on protected rights or intended benefits with isolated lawsuits and/or complaints that do not involve cross-cutting program issues.	Some economic disruption to a metropolitan area or portion of a State, but effects are both manageable and short term
Insignificant or Neutral	Minimal impact on budget/finances/eligibility. Recoverable within current year. Some waste or abuse. Leads to immaterial audit findings.	Isolated local community or individual issue-based concerns	Negligible impact on the effectiveness of the organization. Isolated or short term business service disruption.	Legal issues managed by routine procedures.	Assets receive minimal damage or are only temporarily unavailable or restricted.	Impact can be managed through routine activities.	No measurable impact to the the human and natural environment. No action required for management or containment. No impact to flora, fauna, and or cultural heritage.	Incident with or without minor injury.	No measureable impact to protected rights or intended benefits of individuals.	Some localized, short-term economic disruption

## Likelihood Criteria Matrix

	Staffing (Levels & Experience)	Operational Procedures	Guidance	Problem History	New Program, Phase or Component	Complexity	Outside Control	Potential for Waste, Fraud and Abuse	Work Force Development and Training	FHWA Involvement	Consultant Use	Other
Likelihood Level	Is the FHWA and DOT staff assigned to the effort sufficient? Do they have a clear knowledge, understanding, and ability with the program area or objective and its implications	Are there documented and relevant procedures for this program area or objective of the program?	Is there relevant guidance?	Have there been significant problems or ongoing series of problems related to this program area or objective?	Is program area or objective of the program is truly novel?	Is there a high level of intricacy or challenge associated with the program area or objective?	Is there an opportunity for outside agencies to assert control or interference?	What is the opportunity waste, fraud, and abuse?	Is there program in place to keep training and development in place for the personnel related to this program area or objective?	Is our division office staff actively involved in managing the program area or objective?	Are consultants actively being applied as primary resources in the effort?	Are there other areas of concern related to this program area or objective that are not addressed in the frequency criteria? (Document the criteria below)
Almost Certain	<u>Severely understaffed or no experience:</u> It is unrealistic to expect the staff assigned not to need supplementation or augmentation before the end of the effort	<u>None:</u> There are no documented or relevant procedures	<u>None:</u> There are no documented or relevant guidance	<u>A lot of:</u> There are historical events that tie directly to the problem history	<u>Cutting Edge:</u> No one has addressed this type of work in this program area or objective before	<u>Almost Certain:</u> The program area or objective involves integration of multiple agencies, consultants, contractors and FHWA HQ	<u>Almost Certain:</u> Numerous outside agencies and the public have the opportunity and ability to voice concerns, influence or direct	<u>A lot of:</u> There is almost no oversight and a almost no ability to identify waste, fraud and abuse	<u>None:</u> There are no training or mentoring programs	<u>None:</u> Division office personnel have no visibility or no management control	<u>A lot of:</u> The DOT is using a broad range of consultant to address the program area or objective	
Likely	<u>Understaffed or no experience:</u> Staff assigned will be over utilized and likely incapable of completion of with out immediate training.	<u>Some:</u> There are some documented procedures or tangentially related procedures	<u>Some:</u> There is some documented guidance or tangentially related guidance	<u>Some:</u> There have been some incidents of problems related to this program area or objective in this type of program	<u>Done in other transportation agencies:</u> This type of work has been done in other transportation agencies, but no experience at this agency	<u>Likely:</u> The program area or objective involves integration of multiple agencies and FHWA HQ	<u>Likely:</u> One or two outside agencies and the public have the opportunity and ability to voice concerns, influence or direct	<u>Some:</u> There is some oversight, but certain gaps in our ability to identify waste, fraud and abuse	<u>Limited:</u> There are training and/or mentoring programs, but no funding and/or leadership commitment	<u>Limited:</u> Division office personnel have visibility but no management control	<u>Some:</u> The DOT is sharing significant responsibilities with consultants related to this program area or objective	
Possible	<u>Understaffed or some experience:</u> Staff assigned will be over utilized and run the risk of being incapable of completion if additional responsibilities are assigned, or lack experience	<u>Out-of-date:</u> There are documented procedures, but they are out-of-date with existing laws and regulations.	<u>Out-to-date:</u> There are documented guidance, but they are out-of-date with existing laws and regulations.	<u>Possible:</u> There are rumors or organizational legend of problems related to this program area or objective in this type of program	<u>Some experience:</u> Some people have done this type of work in the past or have done related work	<u>Possible:</u> This program area or objective involves integration of DOT, FHWA and one other outside agency	<u>Possible:</u> One or two outside agencies have the opportunity and ability to voice concerns, influence or direct	<u>Possible:</u> There is oversight, but possible gaps in our ability to identify waste, fraud and abuse	<u>Some:</u> There are training and/or mentoring programs, but they are not universally available	<u>Some:</u> Division office personnel have management control over some aspects of the program area or objective	<u>Limited:</u> The DOT is sharing limited responsibilities with consultants related to this program area or objective	
Unlikely	<u>Adequately staffed or competent:</u> Adequately staffed or competent	<u>Good and up-to-date:</u> Procedures are good and up to date.	<u>Good and up-to-date:</u> Guidance is good and up to date.	<u>None:</u> There have been no significant or ongoing problems.	<u>Old news:</u> It's what we do, routine	<u>Unlikely:</u> This program area or objective involves only DOT and FHWA personnel	<u>Unlikely:</u> There is virtually no opportunity or ability for outside agencies to voice concerns related to this program area or objective	<u>None:</u> There is virtually total oversight and a high opportunity to identify waste, fraud and abuse	<u>A lot of:</u> There are training and mentoring programs, broadly available to FHWA and DOT personnel	<u>A lot of:</u> Division office personnel have active management control over most aspects of the program area or objective	<u>None:</u> The DOT has full responsibility for all aspects of this program area or objective	

## Risk - Heat Map

	Likelihood	Unlikely	Possible	Likely	Almost Certain
Impact	Description	The event could possibly occur, but is unlikely at this time.	The event could occur under specific conditions and some of those conditions are currently evidenced.	The event is most likely to occur in most circumstances.	The event is expected to occur in most circumstances or is happening now.
Catastrophic	Large unacceptable financial loss, severe budget variance. Very significant harm to image with substantial impact on effectiveness. Large and unacceptable operational impact, long term business interruption. Qualified audit finding.				
Major	Very significant financial loss, major budget variance. Major embarrassment leading to significant impact on effectiveness. Unacceptable operational impact, short term business interruption. Leads to material weakness.				
Moderate	Significant financial loss and variance to budget. Moderate embarrassment impacting short term effectiveness. Moderate operational impact, business not interrupted. Leads to reportable findings.				
Minor	Minor financial loss, small budget variance. Minor embarrassment, but no harm to image or reputation. Minor operational impact, business not interrupted. Leads to audit findings.				
Insignificant or Neutral	Minimal or no measurable operational impact. Can be managed with routine activities. Leads to immaterial audit findings.				
<b>How to use this Tool:</b> Assess your risk for levels of impact and likelihood. Find where the two values intersect. Use this intersection value to sort your risks and help with risk prioritization. Use your prioritization to help decide which risks require response strategies.					

## APPENDIX E – GLOSSARY

### **Assessable Unit (AU)**

A division or program office defined by the Unit Risk Profile and Inherent Risk Assessment. These are tools utilized by the Office of the Secretary of Transportation for determining risk on a department scale.

### **Business**

As used on the Impact Matrix, its definition is dependent on the context of the risk and the level of the risk assessment. It can refer to the business operations of the agency, a program office, a division office, or a subunit of them.

### **Communication and Consultation**

The continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders and others regarding the management of risk.

- The information can relate to the existence, nature, form, likelihood, severity, evaluation, acceptability, response or other aspects of the management of risk.
- Consultation is a two-way process of informed communication between an organization and its stakeholders or others on an issue prior to making a decision or determining a direction on a particular issue. Consultation is a process which impacts on a decision through influence rather than power; and an input to decision making, not joint decision making.

### **Community**

As used on the Impact Matrix, its definition is dependent on the context of the risk and the level of the risk assessment. It can refer to the international community, the US public citizenry, the state citizenry or a subdivision of it. It can also refer the professional, business, and special interest communities we operate in. Communities can also be stakeholders.

- American Association of State Highway and Transportation Officials (AASHTO) is an example of a professional community.
- Associated General Contractors (AGC) is an example of a business community that we deal with.
- A special interest community would include environmental groups such as the Sierra Club.

### **Context**

The external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.

#### ***External Context***

The external environment in which the organization seeks to achieve its objectives. External context can include

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organization; and
- relationships with, and perceptions and values of, external stakeholders.

## **Internal Context**

The internal environment in which the organization seeks to achieve its objectives. Internal context can include

- office structure, delegation of authority, governance, roles and responsibilities;
- policies, program and organizational goals and objectives, performance metrics, and the strategies that are in place to achieve them;
- organizational capacity, understood in terms of resources and knowledge (e.g. funds, assets, time, people, processes, systems and technologies);
- the relationships with and perceptions and values of internal stakeholders and the organization's culture;
- information systems, communication flows and decision making processes (both formal and informal);
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual and regulatory relationships.

## **Control**

Any measure that is modifying risk or implementing the risk response.

- Controls include any initiatives, process, policy, device, practice, or other actions which respond to the risk.
- Often times control and response are intermingled in use.
- Controls may not always exert the intended or assumed modifying effect that is why risk monitoring is done.

## **Division Office**

A field office of the FHWA located in each of the 50 states plus Washington D.C. and Puerto Rico. Some divisions may have sub-offices with the state. In addition to these offices, there are three Federal Lands field offices.

## **Event**

An occurrence or change of a particular set of circumstances.

- An event can be one or more occurrences, and can have several causes.
- An event can consist of something not happening.
- An event can sometimes be referred to as an “incident” or “accident”.
- An event without consequences can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

## **Federal Highway Administration (FHWA)**

A modal unit of the U.S. Department of Transportation.

## **Federal Lands Highway (FLH)**

A unit of the Federal Highway Administration consisting of a headquarters office and three field offices (called divisions).



## **Heat Map**

A graphical plot or visual tool used to represent the relative placement of risks. The expected value of the risk determines its location. For example, on a grid, a catastrophic impact and almost certain likelihood risk would be in the upper right quadrant. The heat map can also be used to indicate risk tolerance or residual risk.

## **Impact**

The outcome of an event affecting objectives

- An event can lead to a range of impacts.
- An impact can be certain or uncertain and can have positive (opportunity) or negative (threat) effects on objectives.
- Impacts can be expressed qualitatively or quantitatively.
- Initial impact can escalate through a domino effect.

## **Likelihood**

The chance of something happening.

- In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively. It can be described using general terms (ex. unlikely, probable) or mathematically (such as a probability – 10%, or a frequency over a given time period – 3 times/year).
- For high level risk assessments, probability with any mathematical precision is difficult to do without historical data. New legislation or programs will typically have similar issues.

## **Monitoring**

The continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. Monitoring can also be a communication tool.

- Monitoring can be applied to a risk management framework, risk management process, risk or response.
- For FHWA this is done using by using SUPPS, Risk Tracker, dashboards, or risk registers.

## **Objective**

At the strategic level it is a broad statement of a general direction or result to be achieved. At the division or unit level it is more narrowly defined.

## **Opportunity**

A risk that has positive impact, result, or benefit.

## **Residual/Retained Risk**

Risk remaining after implementing the risk response. In many situations it is not possible or practical to completely eliminate a risk. Residual risk can contain unidentified risk.

## **Review**

An activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. A review can be initiated in response to information

from monitoring activities. It can be done by internal or external (Office of Inspector General, General Accountability Office) entities.

- Review can be applied to a policy, risk management framework, risk management process, risk, or response.
- The breadth, depth, and format of the review will be determined by the purpose and subject of the review.

## **Risk**

Internationally, risk is the “effect of uncertainty on objectives.” In FHWA we define risk as a future event that may or may not occur and has a direct impact on the program, stewardship or organizational objectives, to their benefit or detriment.

- An effect is a deviation from the expected — positive or negative.
- Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, program, project, product, and process).
- Risk is often characterized by reference to potential events and impacts or a combination of these.
- Risk is often expressed in terms of a combination of the impact of an event (including changes in circumstances) and the associated likelihood of occurrence.
- Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its impact, or likelihood.

## **Risk Analysis**

The process to comprehend the nature of risk and to determine the level of risk.

- Risk analysis provides the basis for risk evaluation and decisions about risk treatment.
- Risk analysis includes risk estimation.

## **Risk Assessment**

The overall process of risk identification, risk analysis, and risk evaluation.

## **Risk Attitude**

An organization's or unit's approach to assess and eventually pursue, retain, take or turn away from risk. This can vary across program areas, divisions, or offices. The risk attitude plays into determining the risk response.

## **Risk Aversion**

The attitude to turn away from risk. In some situations the risk may be able to be transferred or avoided. Risk aversion is closely linked to risk attitude.

## **Risk Criteria**

The terms of reference against which the impact, likelihood and significance of a risk is evaluated. Developing the criteria allows for comparison of risk. General criteria typically include such areas as: financial, safety, or environment. At the project level scope, schedule, and budget are typically included.

- Risk criteria are based on organizational objectives, and external and internal context

- Risk criteria can be derived from standards, specifications, laws, policies, and other requirements.

## **Risk Evaluation**

The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk response.

## **Risk Identification**

The process of finding, recognizing and describing risks.

- Risk identification involves the identification of risk sources, events, their causes and their potential impacts.
- Risk identification can involve historical data, theoretical analysis, informed and expert opinions, brainstorming, stakeholder's needs or other methods.

## **Risk Management**

Coordinated activities to direct and control an organization with regard to risk.

## **Risk Management Framework**

The set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

- The foundations include the policy, objectives, mandate and commitment to manage risk.
- The organizational arrangements include plans, tools, relationships, accountabilities, resources, processes and activities.
- The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

## **Risk Management Plan**

Scheme within the risk management framework specifying the response strategies, the management components and resources to be applied to the management of risk.

- Management components typically include procedures, practices, resources, assignment of responsibilities, sequence and timing of activities.
- The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

## **Risk Management Policy**

A high level statement of the overall intentions and direction of an organization related to risk management.

## **Risk Management Process**

The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

## **Risk Owner**

The person or entity within FHWA having the accountability and authority to manage, or responsibility to track the risk.

## **Risk Profile**

A description of any set of risks. The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

## **Risk Response (Risk Response Strategy)**

The process to modify risk. Risk response can involve

- Mitigate the risk. This can involve removing the risk source, reducing the likelihood or reducing the consequences.
- Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk;
- Transfer (or share) the risk to another party or parties
- Accept the risk by informed choice. Use existing controls, process or procedures to deal with the risk should it occur.
- Enhance or exploit risk in order to pursue an opportunity.
- Risk responses that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction” in literature on the subject.
- Risk responses can create new risks or modify existing risks.

## **Risk Source**

An activity, process, project, or program which alone or in combination has the intrinsic potential to give rise to risk. Lack of something can also give rise to risk.

## **Risk Statement**

A two part statement composed of the event and the impact should that event occur. Generally it is forward looking and put in the format of an “If <event> occurs, then <impact> will happen” statement. One event may have multiple impacts.

## **Risk Tracker**

An FHWA risk register application that allows units to track risks and their response strategies. It also provides for consistent categorization and national roll up of unit top risks.

## **Risk Response Tracking System**

See Risk Tracker

## **Shared Unit Performance Plan System (SUPPS)**

A Web-based planning database that is used to house and archive annual unit performance plans, Directors of Field Services dashboard measures data, and related information. Unit-level performance objectives are aligned with the SIP national performance objectives in the SUPPS..

## **Subject Matter Expert (SME)**

An individual or team possessing unique, historical, or specialized knowledge on a subject, program, process, law, regulation, or activity. This knowledge can be formally obtained through education or informally obtained through experience.

## **Stakeholder**

A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. For FHWA stakeholders can be Congress, state departments of transportation, tribes, other federal agencies, regional or metropolitan planning organizations, other local public entities, environmental or civic groups, or individuals.

- A decision maker can be a stakeholder.
- A stakeholder can be internal or external to the organizational unit.

## **Strategic Implementation Plan (SIP)**

An annual plan document, aligned with the FHWA Strategic Plan, that lays out the priority national performance objectives, measures, and initiatives for the coming year.

## **Strategic Plan (SP)**

A multi-year plan document, typically written for a 3-5 year time horizon, that identifies the long term goals, strategic objectives, and national strategies the FHWA will adopt to achieve its vision and mission.

## **Strengths, Weaknesses, Opportunities, and Threats (SWOT or SWOT Analysis)**

A tool or method of collecting and categorizing data about the unit, division, office, or agency for analysis. It is both present and forward looking and includes internal and external assessments..

## **Threat**

A risk that has negative or detrimental impact or result.

## **Unit Performance Plan (UPP)**

An annual plan document developed by a FHWA office to align and support the FHWA SIP. It can contain activities that support division or office goals not defined by the Strategic Plan or Strategic Implementation Plan. An office or division may assign another name to this document (unit action plan) to fit their operating environment.

## **Validation**

A process by which leadership of the unit, office, division, or agency review the risk register or risk evaluation. They may not have been involved in the risk identification process or criteria development. Since this step is done near the end of the process, leadership may have access to information not previously available. The process for this step is situational.